# ELSA MicroLink™ Cable

© 2000 ELSA AG, Aachen (Germany)

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. ELSA haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von ELSA gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

ELSA ist DIN-EN-ISO-9001-zertifiziert. Mit der Urkunde vom 15.06.1998 bescheinigt die akkreditierte Zertifizierungsstelle TÜV-CERT die Konformität mit der weltweit anerkannten Norm DIN EN ISO 9001. Die an ELSA vergebene Zertifikatsnummer lautet 09 100 5069.

Alle Erklärungen und Urkunden zur Zulassung der Produkte finden Sie im Anhang dieser Dokumentation, sofern sie zum Zeitpunkt der Drucklegung vorlagen.

Marken

Windows®, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das ELSA-Logo ist eine eingetragene Marke der ELSA AG. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

ELSA behält sich vor, die genannten Daten ohne Ankündigung zu ändern, und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

ELSA AG

Sonnenweg 11

52070 Aachen

Deutschland

www.elsa.de

Aachen, Juni 2000

20800/0500

# Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Mit dem *ELSA MicroLink Cable* haben Sie sich für ein Modem entschieden, daß Ihnen mit bisher unbekannten Geschwindigkeiten die Tür ins Internet öffnet und dabei permanent online ist.

Höchste Qualitätsanforderungen in der Fertigung und eine enggefaßte Qualitätskontrolle bilden die Basis für den hohen Produktstandard und sind Voraussetzung für gleichbleibende Produktqualität.

In dieser Dokumentation warten die folgenden Kapitel auf Sie:

- Das *ELSA MicroLink Cable* stellt sich vor
- Installation und Inbetriebsnahme
- Konfigurationsmöglichkeiten
- Betriebsarten und Funktionen
- Technische Grundlagen
- Technische Referenz
- Anhang

An der Erstellung dieser Dokumentation haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres ELSA-Produktes anzubieten.

Sollten Sie dennoch einen Fehler finden, oder Sie möchten einfach eine Kritik oder Anregung zu dieser Dokumentation äußern, senden Sie bitte eine E-Mail direkt an:

Cable.doku@elsa.de

*Sollten Sie zu den in der Dokumentation besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.elsa.de rund um die Uhr zur Verfügung. Hier finden Sie im Dateibereich 'Support' unter 'Know-how' viele Antworten auf „häufig gestellte Fragen". Darüber hinaus bietet Ihnen die Wissensdatenbank (KnowledgeBase) einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Handbücher stehen Ihnen jederzeit zum Download bereit.*

*Die KnowledgeBase ist auch auf der CD enthalten. Starten Sie dazu die Datei \Misc\Support\MISC\ELSASIDE\index.htm.*

# Inhalt

**1 *ELSA MicroLink Cable* stellt sich vor . . . . . 9**
1.1 Vorhang auf für *ELSA MicroLink Cable* . . . . . 9
1.1.1 Wie sieht das Gerät aus? . . . . . 9
1.1.2 Node oder Hub? . . . . . 12
1.2 Die Highlights des *ELSA MicroLink Cable* . . . . . 13
1.2.1 Schnelles Internet . . . . . 13
1.2.2 Immer Internet – Immer Online . . . . . 14
1.2.3 Mehr als Internet . . . . . 14

**2 Installation und Inbetriebnahme . . . . . 17**
2.1 Erste Schritte . . . . . 18
2.2 Quick Start: Schnelle Konfiguration . . . . . 19
2.2.1 Vorbereitungen . . . . . 19
2.2.2 Arbeitsplatzrechner unter Windows einrichten . . . . . 20
2.2.3 Die Setup-Assistenten von *ELSA LANconfig* . . . . . 23

**3 Konfigurationsmöglichkeiten . . . . . 25**
3.1 Der komfortable Weg: Inband . . . . . 25
3.1.1 Voraussetzungen für die Inband-Konfiguration . . . . . 25
3.1.2 Alternativ: Adreßverwaltung mit dem DHCP-Server . . . . . 25
3.1.3 Starten der Inband-Konfiguration über *ELSA LANconfig* . . . . . 26
3.1.4 Starten der Inband-Konfiguration über Telnet . . . . . 27
3.2 Befehle für die Konfiguration . . . . . 27
3.3 Konfiguration als Bridge . . . . . 29
3.4 Konfiguration als Router . . . . . 31
3.5 Was ist los auf der Leitung? . . . . . 33
3.5.1 Trace-Ausgaben . . . . . 33
3.6 Neue Firmware mit FirmSafe . . . . . 35
3.6.1 So funktioniert FirmSafe . . . . . 35
3.6.2 So spielen Sie eine neue Software ein . . . . . 36
3.7 Konfiguration über SNMP . . . . . 38
3.7.1 Allgemeines . . . . . 38
3.7.2 Zugriff auf Tabellen und Parameter über SNMP . . . . . 39
3.7.3 Die Management-Information-Base (MIB) . . . . . 40

**4 Funktionen und Betriebsarten . . . . . 41**
4.1 Sicherheit für Ihre Konfiguration . . . . . 41
4.1.1 Paßwortschutz . . . . . 41
4.1.2 Die Login-Sperre . . . . . 42
4.1.3 Zugangskontrolle über TCP/IP . . . . . 42
4.2 Sicherheit für Ihr LAN . . . . . 43
4.2.1 Verschlüsselung . . . . . 43
4.2.2 Filter für die TCP/IP-Pakete . . . . . 43
4.2.3 Das Versteck – IP-Masquerading (NAT, PAT) . . . . . 44
4.3 IP-Routing . . . . . 44
4.3.1 Die IP-Routing-Tabelle . . . . . 45
4.3.2 Dynamisches Routing mit IP-RIP . . . . . 47
4.3.3 Lokales Routing . . . . . 48
4.3.4 IP-Masquerading (NAT, PAT) . . . . . 49
4.3.5 DNS-Forwarding . . . . . 52
4.3.6 Bridging . . . . . 53
4.4 Automatische Adreßverwaltung mit DHCP . . . . . 54
4.4.1 Der DHCP-Client . . . . . 54
4.4.2 Der DHCP-Server . . . . . 55
4.4.3 DHCP – 'Ein', 'Aus' oder 'Auto'? . . . . . 55
4.4.4 So werden die Adressen zugewiesen . . . . . 56

**5 Technische Grundlagen . . . . . 61**
5.1 Die Technik der Kabelmodems . . . . . 61
5.1.1 Standards . . . . . 61
5.1.2 Der Zugang . . . . . 62
5.1.3 Anmeldung im Kabelnetz . . . . . 63
5.2 Netzwerktechnik . . . . . 64
5.2.1 Das Netzwerk und seine Komponenten . . . . . 64
5.2.2 Verbindungsarten . . . . . 65
5.2.3 Netzwerk-Arten . . . . . 67
5.3 IP-Adressierung . . . . . 68
5.3.1 IP-Routing und hierarchische IP-Adressierung . . . . . 71
5.3.2 Erweiterung durch lokale Netze . . . . . 73

**6 Technische Daten . . . . . 79**
6.1 Leistungs- und Kenndaten . . . . . 79
6.1.1 Kabel-TV-Schnittstelle DOCSIS . . . . . 80
6.1.2 Kabel-TV-Schnittstelle EuroDOCSIS . . . . . 81

**7 Anhang . . . . . 83**
7.1 Konformitätserklärung . . . . . 83
7.2 Allgemeine Garantiebedingungen . . . . . 84

**8 Index . . . . . 87**

**Die Menüreferenz für *ELSA MicroLink Cable* gibt es nur auf CD.**

DE

# 1 *ELSA MicroLink Cable* stellt sich vor

Die Hauptanwendung für das *ELSA MicroLink Cable* ist der Zugriff auf das Internet. Der Betreiber des Kabelnetzes, an das Sie Ihr Modem anschließen, kann darüber hinaus auch noch weitere Dienste oder regionale Informationen anbieten.

In diesem Kapitel zeigen wir Ihnen die Anzeige- und Anschlußelemente des Modems, wie der Zugang zum Internet abläuft und mit welchen Eigenschaften und Techniken es den schnellen und sicheren Datenaustausch ermöglicht.

Die genaue Verwendung der *ELSA MicroLink Cable*-Features erläutern wir in den nachfolgenden Kapiteln und anhand der Beispiele im Workshop.

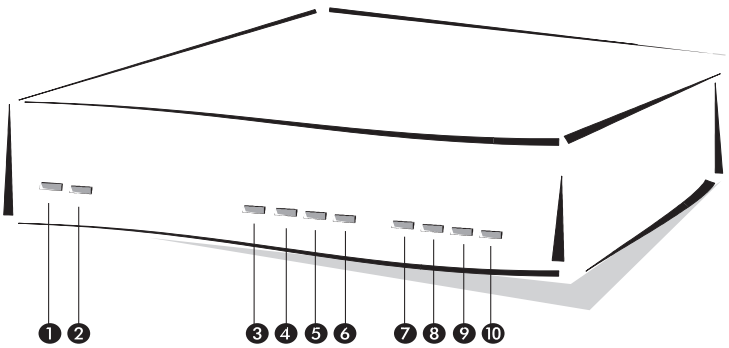
## 1.1 Vorhang auf für *ELSA MicroLink Cable*

In diesem Abschnitt stellen wir Ihnen die Hardware des Geräts vor. Sie erfahren etwas über die Bedeutung der Anzeigeelemente sowie die Anschlußmöglichkeiten.

### 1.1.1 Wie sieht das Gerät aus?

Zunächst wollen wir Sie mit dem Gerät vertraut machen.

An der Vorderseite finden Sie als Anzeigeelemente zehn Leuchtdioden (LEDs).



DE

| | | | |
|---|---|---|---|
| ❶ | On | ❻ | Cable-Reg'd |
| ❷ | Standby | ❼ | LAN-Tx |
| ❸ | Cable-Tx | ❽ | LAN-Rx |
| ❹ | Cable-Rx | ❾ | LAN-Coll |
| ❺ | Cable-Sync | ❿ | LAN-Link |

*ON*

Diese LED wird beim Einschalten der Versorgungsspannung einmal kurz eingeschaltet. Nach dem Selbsttest wird dann entweder ein evtl. festgestellter Fehler als Blinkcode ausgegeben, oder aber das Gerät geht in Betrieb, und die LED leuchtet. Ein sanft pulsendes Leuchten der LED zeigt an, dass das Gerät gerade einen Kanal sucht (ab der neuesten Firmware-Version).

| | | |
|---|---|---|
| aus | | Gerät abgeschaltet, jedoch nicht stromlos |
| rot | 1 x kurz | Bootvorgang (Test und Laden) begonnen |
| rot | blinkend | Anzeige eines Bootfehlers (im Blinkcode kodiert) |
| rot | sanft pulsend | Gerät sucht nach einem Kanal |
| rot | konstant leuchtend | Gerät betriebsbereit |

*Standby*

Diese LED zeigt an, daß sich das Gerät im Standby-Modus befindet. In diesem Zustand ist das *ELSA MicroLink Cable* zwar beim Kabelnetzbetreiber eingebucht, es besteht aber keine Verbindung zum lokalen Netzwerk. In diesem Zustand können also auch keine Daten zwischen Internet und LAN ausgetauscht werden.

Sie schalten das *ELSA MicroLink Cable* in diesen Modus, indem Sie die Funktion des Power-Schalters entsprechend konfigurieren und dann diesen Schalter an der Rückseite des Geräts umlegen. Sie können diese Einstellung auch mit *ELSA LANconfig* vornehmen (Management/Bedienung/Standby).

*Cable-Tx, -Rx, -Sync, Reg'd*

Diese LEDs zeigen die Zustände an der Schnittstelle zum Kabelnetz an:

| | | |
|---|---|---|
| Cable-Tx | gelb | Datenpaket vom Gerät an das Internet gesendet |
| Cable-Rx | grün | Datenpaket aus dem Internet empfangen |
| Cable-Sync | grün | Das Gerät hat einen Kanal gefunden, auf dem es mit dem Head-End beim Kabelnetzbetreiber kommunizieren kann. |

| | | |
|---|---|---|
| Cable-Reg'd | grün | Die Registrierung mit allen notwendigen Verhandlungen zwischen dem Gerät und dem Head-End sind abgeschlossen, die Registrierung wurde vom Head-End bestätigt. In diesem Zustand ist das Gerät bereit, Daten mit dem Internet auszutauschen. |

*Blinkcodes*

Die beiden LEDs Sync und Reg'd können durch kombinierte Blink-Codes die verschiedenen Phasen bei der Anmeldung des Kabelmodems darstellen und so Hinweise für die Fehlersuche bei der Konfiguration geben. Die verschiedenen Blinkcodes bedeuten im einzelnen:

| **SYNC** | **REG'd** | **Was ist bis jetzt erreicht?** | **Was versucht das Modem?** |
|---|---|---|---|
| aus | aus | | Kanal-Suche mit 64/256QAM-Kanal |
| 1 Puls | aus | QAM-Lock | FEC-Lock |
| 2 Pulse | aus | FEC-Lock | TRC-Lock |
| an | aus | TRC-Lock | initial Ranging |
| an | 1 Puls | initial Ranging | DHCP |
| an | 2 Pulse | DHCP | ToD |
| an | 3 Pulse | ToD | Configuration File |
| an | 4 Pulse | Configuration File | Registrierung |
| an | 5 Pulse | Registrierung | Kryptifizierung |
| an | an | Registrierung (evtl. mit Kryptifizierung) | |

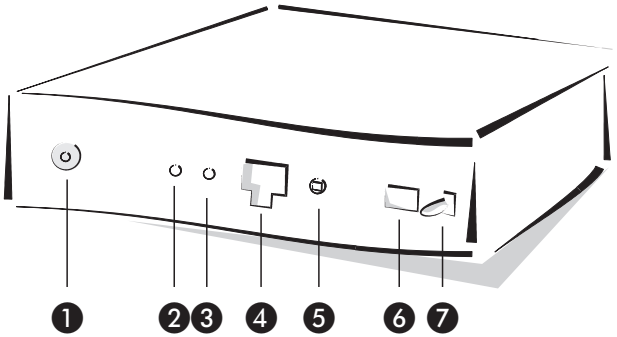
*LAN-Tx, -Rx, LAN-Coll, -Link*

Diese LEDs zeigen die entsprechenden Zustände des Netzwerk-Controllers an:

| | | |
|---|---|---|
| LAN-Tx | gelb | Datenpaket vom Gerät an das LAN gesendet |
| LAN-Rx | grün | Datenpaket aus dem LAN empfangen |
| LAN-Coll | rot | Sendekollision |
| LAN-Link | grün | Der Anschluß zum LAN ist hergestellt und bereit |

DE

Jetzt drehen Sie das Ganze mal um und sehen sich die Rückseite an. Wieder von links finden Sie:




1. Anschluß für das TV-Kabelnetz (CATV)
2. Reset-Taster, führt einen Harware-Reset durch
3. Factory-Default-Taster, setzt das Gerät in den Auslieferungszustand zurück (nach ca. 10–15 s Drücken).
4. 10Base-T-Netzwerkanschluß
5. Node/Hub-Umschalter
6. Anschluß für das Netzteil
7. Ein/Standby-Schalter

### 1.1.2 Node oder Hub?

Beachten Sie beim Anschluß an das Netzwerk die Stellung des Node/Hub-Umschalters:

- Im Auslieferungszustand steht der Umschalter auf 'Hub'. In dieser Stellung verhält sich das Kabelmodem wie ein Hub und kann direkt an die Netzwerkkarte des Rechners angeschlossen werden. Die Leitungen zum Senden und Empfangen der Daten werden in dieser Stellung gekreuzt.
- Stellen Sie den Umschalter auf 'Node' um, wenn Sie das Gerät an einen Hub anschließen wollen.

*Sie können die korrekte Stellung des Node/Hub-Umschalters mit Hilfe der Link-Status-LED (Link) überprüfen.*

DE

## 1.2 Die Highlights des *ELSA MicroLink Cable*

Mit ihrer neuen Zugangstechnologie zum Internet treten Kabelmodems in Konkurrenz zu normalen Modems, Internet-Modems und kleinen ISDN-Routern. Um Ihr *ELSA MicroLink Cable* richtig nutzen zu können, sollten Sie wissen, in welchen Bereichen die Kabelmodems in diesem Wettbewerb die Nase vorn haben bzw. welche Eigenschaften Sie den anderen Geräten voraus haben.

### 1.2.1 Schnelles Internet

Bei den Kabelmodems gibt es eine asymetrische Teilung der Übertragungsraten je nach Senderichtung. Downstream bezeichnet die Übertragung vom Netzbetreiber zum Teilnehmer, Upstream die entgegengesetzte Richtung. Die asymetrische Teilung ist auch durchaus sinnvoll, denn i.d.R. holen die Nutzer des Internets deutlich mehr Informationen aus dem Web ab als sie selbst hineinsenden.

#### Kabelnetz

Im Downstream können bis 43 Mbit/s übertragen werden, im Upstream immerhin 10 Mbit/s.

***Shared Media**: Viele Nutzer teilen sich ein „Kabel"*

Diese gigantische Leistung teilen sich allerdings bis zu 2000 Benutzer, die gemeinsam an einem Kabelstrang angeschlossen sind. Man spricht auch von der Nutzung von Shared Media.

***Bandbreite**: Datenrate, Übertragungskapazität*

Da der Datenfluß bei der Nutzung des Kabelnetzes jedoch nicht kontinuierlich gleich ist, sondern in unregelmäßigen zeitlichen Intervallen abläuft, und darüber hinaus wohl kaum alle 2000 Benutzer gleichzeitig das Netz nutzen möchten, ist die verfügbare Bandbreite auf jeden Fall ausreichend für schnelle Datenübertragung.

Die Kabelnetzbetreiber haben die Möglichkeit, die verfügbare Bandbreite für die einzelnen Teilnehmer einzuschränken oder mehrere Kanäle mit jeweils 43 Mbit/s anzubieten. Erkundigen Sie sich also bei Ihrem Netzbetreiber, welche Übertragungsraten er in welchem Tarifmodell einräumt.

#### Backbone

***Backbone**: direkte Verbindung ins Internet*

Die reine Übertragungsrate zwischen Netzbetreiber und Teilnehmer bestimmt allerdings nicht alleine die Zugriffsgeschwindigkeit auf das Internet. Der Netzbetreiber muß den für das Internet bestimmten Datenstrom noch einmal in einen Backbone weiterleiten. Von der Auslegung dieses

Anschlusses hängt es ab, wie schnell Sie letztendlich im Internet surfen können. Wenn viele Teilnehmer gleichzeitig Daten aus dem Internet abrufen wollen, und der Netzbetreiber eine nicht ausreichend dimensionierte Leitung ins Internet hat, kann der Backbone zum Nadelöhr werden.

### 1.2.2 Immer Internet – Immer Online

Einer der größten Vorteile der Kabelmodemtechnik ist die permanente Verfügbarkeit des Internets. Während bei „normalen" Internet-Zugängen bei Bedarf erst eine Verbindung zum Internet hergetellt werden muß, können beim Kabelmodem alle Teilnehmer eines Kabelnetzabschnitts permanent beim Head-End eingebucht sein. Durch die Multiportfähigkeit der Gegenstellen werden dabei auch keine anderen Teilnehmer blockiert, für die dann evtl. keine Zugänge mehr vorhanden wären. Die Vorteile dieser permanenten Internet-Anbindung:

- Unmittelbare Verfügbarkeit aller Informationen

  Ihre E-Mails kommen direkt zu Ihnen, nicht nur dann, wenn Sie sie abholen. Wenn Sie eine Web-Seite ansehen möchten, starten Sie nur Ihren Browser und kümmern sich nicht um die Verbindung zum Provider.

- Eigener Server im Internet

  Bisher brauchte man für einen eigenen Server im Internet u.a. eine (sehr teure) Standleitung zum Provider. Die haben Sie jetzt! Wenn Sie also einen eigenen Web-Server in Ihrer Firma aufbauen wollen, ist dieser über das Kabelmodem erreichbar.

### 1.2.3 Mehr als Internet

Kabelmodems bilden zusammen mit den entsprechenden Gegenstellen die Verbindung zwischen Netzteilnehmer (privat oder geschäftlich) und dem Netzbetreiber. Auf dieser Strecke können sehr hohe Übertragungsraten und damit sehr schnelle Datenübertragungen erreicht werden. Das eröffnet neben dem schnellen Zugang zum Internet weitere interessante Möglichkeiten, mit denen sich die Kabelnetzbetreiber zu Informationsdienstleistern mausern können.

#### Regionale Inhalte

Die Kabelnetzbetreiber haben aufgrund der Struktur des Kabelnetzes meist eine regionale oder lokale Ausrichtung. Mit den auf ca. 2000 Teilnehmer

begrenzten Head-Ends, die zusätzlich in das Netz eingebracht werden, entstehen zusätzlich räumlich sehr begrenzte Schaltstellen.

Diese Struktur kann der Netzbetreiber dazu nutzen, regionale Inhalte zusätzlich zum Internet anzubieten. Dazu richtet er in seinem eigenen Netz Web-Server ein, die im Internet nicht erreichbar sein müssen. Darauf kann er dann ein spezielles Informationsangebot für seine Teilnehmer bereitstellen, wie z.B. lokales Kinoprogramm, regionale Nachrichten, Vereinsinformationen etc. Eben alles, was die Teilnehmer im eigenen Netz interessiert, im World Wide Web aber vielleicht überflüssig wäre.

### Proxy-Server

Mit den lokalen Servern kann der Netzbetreiber aber auch den Zugang zum Internet schneller machen. Dazu richtet er Proxy-Server ein, auf denen die Informationen aus dem Internet zwischengespeichert werden.

***Proxy***:
*Stellvertreter*

Jede Seite, die aus dem Web von einem Teilnehmer aus dem lokalen Kabelnetzabschnitt aufgerufen wird, wird auf diesem Proxy-Server abgelegt und bleibt für eine bestimmte Zeit dort liegen. Die Verweildauer auf dem Proxy-Server wird in der Regel vom Kabelnetzbetreiber eingestellt. Wenn dann ein anderer Teilnehmer die gleiche Seite aufruft, kann der Proxy-Server diese Information direkt liefern und muß nicht erst im Internet danach suchen.

Dieses Verfahren hat für die meisten Fälle durchaus Vorteile, weil damit z.B. Downloads sehr viel schneller erledigt werden können. Wenn Sie jedoch sich schnell ändernde Daten abrufen möchten (z.B. Börsenkurse), sind Sie wahrscheinlich auf aktuelle Web-Seite angewiesen. In diesem Fall kann die zwischengespeicherte Version auf dem Proxy-Server veraltet und ggf. falsch sein. Erkundigen Sie sich daher bei Ihrem Netzbetreiber, ob er Proxy-Server einsetzt. Mit einem Klick auf die Schaltfläche **Aktualisieren** in Ihrem Web-Browser können Sie aber die originale Information direkt aus dem Internet laden.

DE

# 2 Installation und Inbetriebnahme

Dieses Kapitel wird Ihnen helfen, möglichst schnell online zu gehen. Bitte prüfen Sie zunächst die Vollständigkeit des Lieferumfangs:

- *ELSA MicroLink Cable*
- Netzteil
- LAN-Anschlußkabel, Twisted-Pair
- Anschlußkabel für TV-Kabelnetz (Koaxial-Kabel) oder entsprechender Adapter
- Dokumentation
- CD mit *ELSA LANconfig* und elektronischer Dokumentation

Die Rechner, die Sie mit Hilfe des Gerätes an das Internet anschließen möchten, müssen folgende Voraussetzung erfüllen:

- beliebiges Betriebssystem, auf dem das Netzwerkprotokoll TCP/IP läuft, z.B. Windows 95, Windows 98, Windows 2000, Windows NT 4.0, OS/2, Linux, BeOS
- Windows 95, Windows 98, Windows 2000 oder Windows NT 4.0 und ein CD-ROM-Laufwerk für die Rechner, auf denen Sie die Konfigurationssoftware *ELSA LANconfig* installieren möchten.
- Ethernet-Netzwerkkarte
- Netzwerkprotokoll TCP/IP, installiert und auf die Netzwerkkarte gebunden

Wir zeigen Ihnen zunächst, wie Sie Ihr neues *ELSA MicroLink Cable* anschließen, wie Sie die Konfigurationssoftware *ELSA LANconfig* installieren und die ersten Konfigurationen durchführen. Danach ist Ihr Gerät schon bereit, Ihren Rechner oder Ihr lokales Netzwerk mit dem Internet zu verbinden.

Wenn Ihnen das alles hier zu schnell geht oder Sie bei den Fachbegriffen nur noch „Bahnhof" verstehen, finden Sie natürlich in dieser Dokumentation auch weitere Informationen (ausführliche Beschreibung des Geräts und seiner Funktionen, Konfigurationsbeispiele, Software-Beschreibungen, Glossar etc.).

*Dieses Gerät ist für den Anschluß an das Breitband-TV-Kabelnetz vorgesehen.*

DE

## 2.1 Erste Schritte

① **Ran an den Strom**

Versorgen Sie Ihr Gerät zunächst über das Netzteil mit der nötigen Spannung!

② **Rein ins Netz**

Verbinden Sie das Gerät über das Twisted-Pair-Kabel mit dem lokalen Netzwerk. Beachten Sie die Stellung des Node/Hub-Umschalters: 'Node' wenn Sie das Gerät am Netzwerk anschließen, 'Hub' wenn Sie es direkt an einen Arbeitsplatzrechner anschließen.

③ **Der Draht nach draußen**

Schließen Sie das *ELSA MicroLink Cable* mit dem Koaxial-Kabel oder mit dem Adapter und einem normalen Antennenkabel an das TV-Kabelnetz an. Die Daten werden im TV-Kabelnetz nach dem DOCSIS-Standard (**D**ata **O**ver **C**abel **S**ystem **I**nterface **S**pecification) übertragen.

*Der Anschluß an das TV-Kabelnetz muß einen bestimmten Signalpegel aufweisen. Dieser Wert wird von Ihrem Kabelnetzbetreiber geprüft und ggf. richtig eingestellt.*

④ **Los geht's**

Schalten Sie das Gerät an der Rückseite ein. Nach einem kurzen Selbsttest leuchtet die LED 'Power' an der Frontseite auf. Die LED 'LAN-Link' zeigt an, daß Ihr Gerät korrekt mit dem LAN verbunden ist und daß der Node/Hub-Umschalter richtig eingestellt ist.

*Falls diese LED nicht leuchten sollte, schalten Sie den Node/Hub-Umschalter um. Falls die LED dann noch immer nicht leuchtet, liegt evtl. ein Problem mit der Netzwerkarte oder der Verkabelung vor.*

⑤ **Software installieren**

Sie können jetzt direkt mit dem Kabelmodem arbeiten, ohne weitere Einstellungen vorzunehmen.

Wenn Sie die Konfiguration des Geräts anpassen und auf andere Anwendungen einstellen wollen, können Sie die Konfigurationssoftware *ELSA LANconfig* für Windows 95, Windows 98, Windows 2000 oder Windows NT 4.0 verwenden. Alternativ können Sie von jedem anderen TCP/IP-fähigen Rechner (z.B. Linux, Solaris) die Konfiguration auch per

Telnet durchführen. Installieren Sie zuerst das Netzwerkprotokoll TCP/IP und anschließend *ELSA LANconfig* auf dem Rechner, von dem aus Sie Ihr Gerät einstellen möchten. Wenn das Setup-Programm beim Einlegen der CD nicht automatisch startet, klicken Sie im Explorer von Windows einfach auf die 'autorun.exe' auf der *ELSA MicroLink Cable* und folgen den Hinweisen der Installationsroutine.

⑥ ***ELSA MicroLink Cable* konfigurieren**

Beim ersten Start von *ELSA LANconfig* wird das neue Gerät automatisch im TCP/IP-Netz erkannt und konfiguriert.

Bei der Konfiguration mit *ELSA LANconfig* können Sie die Setup-Assistenten verwenden, die Sie schnell und komfortabel durch die notwendigen Einstellungen führen.

## 2.2 Quick Start: Schnelle Konfiguration

Nach der Installation der Hardware und der Software wollen Sie natürlich schnell loslegen und sich erst mal nicht um die tieferen technischen Details kümmern. Darum zeigen wir Ihnen in den folgenden Abschnitten, wie Sie Ihr *ELSA MicroLink Cable* in Windeseile auf die gebräuchlichsten Anwendungen einstellen, ohne Sie mit dem Wieso und Warum aufzuhalten.

Nach den Vorbereitungen, die Sie auf jeden Fall prüfen sollten, können Sie mit Hilfe der Assistenten das Gerät direkt in Betrieb nehmen. Weitere Informationen zu den Funktionen von Bridge und Router finden Sie im Kapitel 'Funktionen und Betriebsarten'.

### 2.2.1 Vorbereitungen

Das Internet basiert auf dem Netzwerkprotokoll TCP/IP. Die einzelnen Geräte im Internet (Arbeitsplatzrechner, Server, Router etc.) werden über eindeutige Adressen, die IP-Adressen, identifiziert. Alle Rechner, die am Datenaustausch im Internet teilnehmen möchten, müssen also zum einen mit dem Netzwerkprotokoll TCP/IP ausgerüstet sein und andererseits über eine gültige IP-Adresse verfügen.

Die IP-Adressen können Sie entweder in jedem Rechner von Hand fest eintragen oder Sie lassen die Adresse von einem anderen Rechner, einem DHCP-Server, automatisch zuweisen. Ein solcher DHCP-Server steht bei Ihrem Kabelnetzbetreiber, und das *ELSA MicroLink Cable* bietet diese optionale Erweiterung ebenfalls. Für den Schnelleinstieg bevorzugen wir das automa-

DE

tische Zuweisen der IP-Adressen von einem DHCP-Server an die Rechner. Bei der Vorgabe-Konfiguration als Bridge wird der DHCP-Server des Kabelnetzbetreibers genutzt, in der Betriebsart als Router der eingebaute DHCP-Server im *ELSA MicroLink Cable*.

Unabhängig von der Betriebsart, in der Sie Ihr *ELSA MicroLink Cable* betreiben möchten, sind folgende Einstellungen erforderlich:

- Installieren Sie das Netzwerkprotokoll TCP/IP auf allen Rechnern in Ihrem Netz.
- Aktivieren Sie auf den Rechnern das automatische Beziehen der IP-Adressen über DHCP (meistens so voreingestellt).
- Starten Sie den Setup-Assistenten für den Router-Betrieb, wenn Sie das *ELSA MicroLink Cable* als Router konfigurieren möchten.

## 2.2.2 Arbeitsplatzrechner unter Windows einrichten

### Windows 98 und Windows 95

Am Beispiel von Windows 95 und Windows 98 zeigen wir hier kurz, was Sie zur einwandfreien Kommunikation der Rechner im TCP/IP-Netz mit dem Router auf den Arbeitsplatzrechnern einrichten müssen, falls es nicht schon erledigt ist.

- TCP/IP installieren

  Installieren Sie TCP/IP mit **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ Hinzufügen ▶ Protokoll**. Wählen Sie als Hersteller 'Microsoft' und als Netzwerkprotokoll 'TCP/IP'.

- IP-Adressen zuweisen lassen (DHCP verwenden)

  So stellen Sie die Arbeitsplatzrechner auf das automatische Beziehen der IP-Adressen ein: **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ TCP/IP ▶ Eigenschaften ▶ IP-Adresse ▶ IP-Adresse automatisch beziehen**. Löschen Sie außerdem evtl. vorhandene Einträge für DNS-Server und Gateways (auf den Registerkarten 'Gateway' und 'DNS-Konfiguration' und deaktivieren Sie die Option 'DNS'. Der Rechner sucht dann nach dem Neustart einen DHCP-Server im Netz und läßt sich von diesem eine IP-Adresse und eine Netzmaske zuweisen.

DE

- Feste IP-Adressen einstellen (kein DHCP verwenden)

  Wenn Sie keinen DHCP-Server in Ihrem Netz verwenden möchten, stellen Sie an den Arbeitsplatzrechnern feste IP-Adressen ein: **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ TCP/IP ▶ Eigenschaften ▶ IP-Adresse ▶ IP-Adresse festlegen**.

  Vergeben Sie eindeutige IP-Adressen, z.B. aus einem reservierten Adreßbereich. Die Arbeitsplatzrechner können z.B. die Adressen '10.1.1.2' bis '10.1.1.253' bekommen, das *ELSA MicroLink Cable* die '10.1.1.1', alle mit der Netzmaske '255.255.255.0'. Ob die für das *ELSA MicroLink Cable* vorgesehene IP-Adresse frei ist, z.B. die '10.1.1.1', testen Sie in der DOS-Box durch Eingabe des Kommandos `ping 10.1.1.1`. Wenn Sie auf diese Anfrage keine Antwort erhalten, ist die Adresse wahrscheinlich noch frei.

*Stellen Sie die festen IP-Adressen nur im Routerbetrieb mit aktiviertem IP-Masquerading ein. Im Routerbetrieb ohne IP-Masquerading oder im Bridge-Betrieb kann es sonst zu Adreßkonflikten mit anderen Teilnehmern in Ihrem Kabelnetz kommen. Beachten Sie im Routerbetrieb, daß Sie LAN-seitig nur ein Netzwerk konfigurieren, das vom TV-Kabelnetz verschieden ist.*

### Gateway und DNS-Server eintragen (nicht nötig bei Verwendung von DHCP)

Tragen Sie die LAN-IP-Adresse aus dem *ELSA MicroLink Cable* im eigenen lokalen Netz als Gateway bei den Arbeitsplatzrechnern ein: **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk ▶ TCP/IP ▶ Eigenschaften ▶ Gateway** und **DNS-Konfiguration**.

- Überprüfung der IP-Konfiguration

  Unter Windows 95 oder Windows 98 können Sie mit **Start ▶ Ausführen ▶ winipcfg** die aktuelle IP-Konfiguration des Rechners abfragen. Hier können Sie u.a. sehen, welche IP-Adresse der DHCP-Server dem Rechner zugewiesen hat und welche Adressen für DNS-Server und Gateway übermittelt wurden.

DE

### Windows 2000

Unter Windows 2000 unterstützen Sie hilfsbereite Hardware-Assistenten bei der Installation der neuen Hardware. Falls Ihre Netzwerkkarte nicht schon beim Systemstart erkannt wurde, starten Sie mit

**Start ▶ Einstellungen ▶ Systemsteuerung ▶ Hardware**

den Hardware-Assistenten.

① Bestätigen Sie zunächst den Suchvorgang nach neuen Komponenten, wählen Sie aus der folgenden Liste den Punkt 'Neues Gerät hinzufügen', und klicken Sie auf **Weiter >**.

② Nach dem Suchvorgang sollte die Netzwerkkarte erkannt worden sein. Klicken Sie erneut auf **Weiter >**. Damit ist die neue Hardware und eine LAN-Verbindung eingerichtet.

③ Um die neue LAN-Verbindung zu kontrollieren, öffnen Sie mit

**Start ▶ Einstellungen ▶ Netzwerk- und DFÜ-Verbindungen**

das entsprechende Fenster. Klicken Sie mit der rechten Maustaste auf das Symbol und rufen Sie die 'Eigenschaften' auf.

④ In dem darauffolgenden Dialog sehen Sie ein Listenfenster mit den installierten Netzwerkkomponenten. In dieser Liste sollte in jedem Fall TCP/IP aufgeführt sein.

⑤ Markieren Sie diesen Eintrag, und klicken Sie auf die Schaltfläche **Eigenschaften...**.

In dem folgenden Dialogfenster können Sie alle Eigenschaften für das Netzwerkprotokoll festlegen. Die Vorgehensweise für die Adreßeinstellungen, DHCP, Gateway und DNS sind nach der gleichen Vorgehensweise wie bei Windows 98 vorzunehmen.

- Überprüfung der IP-Konfiguration

  Unter Windows 2000 können Sie mit dem Befehl `ipconfig /all` im DOS-Fenster die aktuelle IP-Konfiguration des Rechners abfragen. Hier können Sie u.a. sehen, welche IP-Adresse der DHCP-Server dem Rechner zugewiesen hat und welche Adressen für DNS-Server und Gateway übermittelt wurden.

### 2.2.3 Die Setup-Assistenten von *ELSA LANconfig*

Um das *ELSA MicroLink Cable* schnell in Betrieb zu nehmen, müssen Sie keine aufwendigen Einstellungen in der Konfiguration vornehmen. In der Voreinstellung ist das Kabelmodem als Bridge konfiguriert. Den Setup-Assistenten rufen Sie nur dann auf, wenn Sie das Kabelmodem als Router betreiben möchten:

① Markieren Sie das zu konfigurierende Gerät im Listenfenster, und starten Sie im Menü **Extras** den **Setup Assistent**.

② Wählen Sie 'Bridge-Betrieb' oder 'Router-Betrieb'. Für den Bridge-Betrieb benötigt der Assistent keine weiteren Angaben von Ihnen. Für den Router-Betrieb wird die IP-Adresse und die Subnetz-Maske abgefragt. Für die schnelle Inbetriebnahme können Sie die Vorgabewerte übernehmen. Einzelheiten hierzu finden Sie im Kapitel 'Konfigurationsmöglichkeiten'.

DE

# 3 Konfigurationsmöglichkeiten

Kabelmodems von ELSA werden immer mit einer aktuellen Software ausgeliefert, in der schon einige Einstellungen für Sie vorbereitet sind.

In diesem Kapitel zeigen wir Ihnen, mit welchen Programmen und über welche Wege Sie auf das Gerät zugreifen können, um die Einstellungen vorzunehmen.

Und wenn das Entwickler-Team eine neue Firmware mit neuen Features für Sie fertiggestellt hat, finden Sie hier Hinweise zum Laden der neuen Software.

## 3.1 Der komfortable Weg: Inband

Mit der Inband-Konfiguration haben Sie von jedem Rechner aus dem LAN Zugriff auf das Gerät. Allerdings nur, wenn er dies zuläßt, denn der Zugang aus dem LAN kann über die IP-Zugangsliste eingeschränkt oder ganz gesperrt werden. Für die Inband-Konfiguration verwenden Sie entweder Telnet (gehört zum Lieferumfang der meisten Betriebssysteme) oder das Konfigurationsprogramm *ELSA LANconfig* für Windows. *ELSA LANconfig* ist im Lieferumfang Ihres Geräts enthalten. Aktuelle Versionen stehen immer in unseren Online-Medien für Sie bereit.

### 3.1.1 Voraussetzungen für die Inband-Konfiguration

Die Konfiguration mit Telnet oder *ELSA LANconfig* läuft über TCP/IP bzw. TFTP ab. Dazu muß also auf dem verwendeten Rechner das TCP/IP installiert sein, und Ihr Kabelmodem benötigt eine IP-Adresse, mit der Sie es ansprechen können.

Ein noch nicht konfiguriertes Gerät hört auf die IP-Adresse XXX.XXX.XXX.254. Die vielen X stehen dabei für die Netzwerkadresse in Ihrem LAN. Haben die Rechner in Ihrem Netz also z.B. Adressen wie 192.110.130.1, dann können Sie Ihr Gerät mit der Adresse 192.110.130.254 erreichen.

*Haben Sie bereits einen Rechner mit der Adresse XXX.XXX.XXX.254 in Ihrem Netz stehen, schalten Sie zunächst den Rechner mit dieser IP-Adresse aus.*

### 3.1.2 Alternativ: Adreßverwaltung mit dem DHCP-Server

Wenn die Konfiguration der korrekten IP-Adressen „von Hand" keine absolute Notwendigkeit für Sie ist, erledigt der DHCP-Server diese Arbeit auch

DE

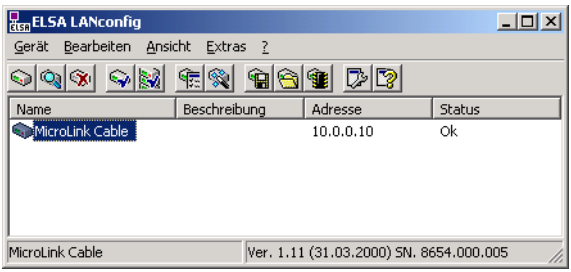
gerne selbständig für Sie. Bei der Verwendung des DHCP-Servers können Sie die IP-Adressen für alle Rechner im Netz automatisch einstellen lassen (siehe auch Kapitel 'Automatische Adreßverwaltung mit DHCP' auf Seite 54).

### 3.1.3 Starten der Inband-Konfiguration über *ELSA LANconfig*

Nach der Installation (mit Doppelklick auf die 'autorun.exe') rufen Sie *ELSA LANconfig* z.B. aus der Windows-Startleiste auf mit **Start** ▶ **Programme** ▶ **ELSAlan** ▶ ***ELSA LANconfig***. *ELSA LANconfig* sucht nun automatisch im lokalen Netz nach *ELSA MicroLink Cable*-Geräten.

Um die Suche eines neuen Geräts manuell einzuleiten, klicken Sie nur auf die Schaltfläche **Suchen** oder rufen den Befehl über **Gerät** ▶ **Suchen** auf. *ELSA LANconfig* erkundigt sich dann, wo es suchen soll. Bei der Inband-Lösung reicht hier die Auswahl des lokalen Netzes, und los geht's.

Sobald *ELSA LANconfig* mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.



Ein Doppelklick auf den Eintrag für das markierte Gerät, der Klick auf die Schaltfläche **Konfigurieren** oder den Menüeintrag **Bearbeiten** ▶ **Konfiguration bearbeiten** liest die aktuellen Einstellungen aus dem Gerät aus und zeigt die allgemeinen Geräteinformationen.

Die weitere Bedienung des Programms erklärt sich im Prinzip selbst bzw. über die Online-Hilfe. Mit einem Klick auf das Fragezeichen oben rechts in jedem Fenster bzw. mit einem rechten Mausklick auf einen unklaren Begriff können Sie jederzeit die kontextsensitive Hilfe aufrufen.

DE

### 3.1.4 Starten der Inband-Konfiguration über Telnet

Über Telnet starten Sie die Inband-Konfiguration z.B. aus einer DOS-Box mit dem Kommando:

```
telnet 10.0.0.10
```

Telnet baut dann eine Verbindung zum Gerät mit der eingegebenen IP-Adresse auf. Wenn die Gerätekonfiguration durch ein Paßwort geschützt wurde, werden Sie nun zur Paßworteingabe aufgefordert.

## 3.2 Befehle für die Konfiguration

Bei der Verwendung von Telnet oder einem Terminalprogramm zur Konfiguration geben Sie Befehle und Pfadangaben so ein, wie Sie es von DOS oder UNIX her kennen.

Zur Trennung der Einträge für einen Pfad geben Sie einen Schrägstrich oder einen umgekehrten Schrägstrich ein. Befehle und Tabelleneinträge müssen nicht vollständig ausgeschrieben werden, eine eindeutige Abkürzung reicht aus.

Bei der Konfiguration werden Einträge der Gruppen MENÜ, WERT, TABELLE, TABINFO, AKTION und INFO angezeigt und evtl. geändert. Die folgenden Befehle können Sie dazu verwenden:

| Dieser Befehl ... | ... hat folgende Bedeutung ... | ... z.B.: |
|---|---|---|
| ? oder help | ruft Hilfetexte auf. | - |
| dir, list, ll, ls <MENÜ>, <WERT> oder <TABELLE> | zeigt den Inhalt von MENÜ, WERT oder TABELLE an. | dir/status/wan-statistik zeigt die aktuelle WAN-Statistik. |
| cd <MENÜ> oder <TABELLE> | wechselt in das angegebene MENÜ oder die TABELLE. | cd setup/tcp-ip-modul (kurz cd se/tc) wechselt in das TCP/IP-Modul. |
| set <WERT> | So setzen Sie den WERT neu. | set ip-adresse 192.110.120.140 setzt eine neue IP-Adresse. |
| | Bei Tabellenzeilen geben Sie alle Einträge getrennt durch Leerzeichen ein. Ein * läßt den Eintrag unverändert. | set /setup/name AACHEN gibt dem Gerät den Namen 'AACHEN' |

| Dieser Befehl ... | ... hat folgende Bedeutung ... | ... z.B.: |
|---|---|---|
| set <WERT> ? | zeigt Ihnen, welche Werte Sie hier eingeben können. | |
| del <WERT> | löscht den Eintrag BAND1 aus der benutzerprogrammierbaren Frequenztabelle | del /se/cab/tun/ban/ BAND1 |
| do <AKTION> (Parameter) | führt die AKTION aus, evtl. mit den angegebenen Parametern. | do /firmware/firmware-upload startet das Einspielen einer neuen Firmware. |
| passwd | erlaubt die Eingabe eines neuen Paßwortes. Hierzu muß, falls vorhanden, zuerst das alte Paßwort eingegeben werden. Danach muß das neue Paßwort zweimal hintereinander eingegeben und jeweils mit ↵ bestätigt werden. | |
| repeat <sek> <AKTION> | zeigt jede Sekunde den Zustand während der Anmeldung am Head-End. | repeat 1 dir /status/ini |
| language <Sprache> | setzt die Sprache der aktuellen Konfigurationssitzung. | Unterstützte Sprachen sind z.Zt.<br>Englisch (language english)<br>Deutsch (language deutsch) |
| exit, quit, x | Konfiguration wird beendet. | |

Textuelle Eingaben mit Leerzeichen werden nur in Anführungszeichen akzeptiert, z.B.

```
set /se/snmp/admin "Der Administrator".
```

Textuelle Einträge (Einzel- und Tabellenwerte) werden wie folgt gelöscht:

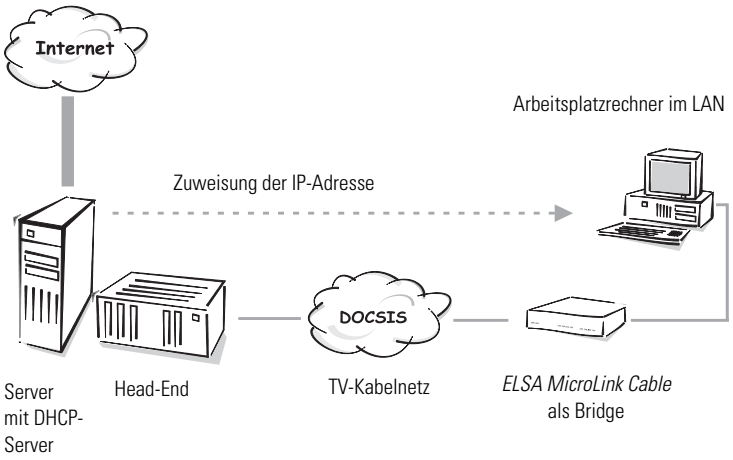
```
set /se/snmp/admin ""
```

DE

## 3.3 Konfiguration als Bridge

*Mit ELSA LANconfig rufen Sie einfach den entsprechenden Setup-Assistenten im Menü 'Extras' auf. Er ermöglicht eine schnelle und komfortable Konfiguration des Kabelmodems. In diesem Abschnitt beschreiben wir die „manuelle Methode" Schritt für Schritt.*

Die Betriebsart als Bridge ist die einfachste Konfiguration für das *ELSA MicroLink Cable* und mit der Auslieferung des Gerätes voreingestellt. Im Bridge-Betrieb achtet das Gerät nicht auf die IP-Adressen und überträgt alle Daten, die nicht an Rechner im eigenen lokalen Netz gerichtet sind, direkt ins Internet. Umgekehrt werden auch alle Daten weitergegeben, die aus dem Internet an einen Rechner im eigenen lokalen Netz gerichtet sind (sofern dieser Rechner vorher selbst schon einmal Daten ins Internet geschickt hat). Sie brauchen sich daher auch nicht um die Zuweisung der IP-Adressen zu kümmern. Die Rechner in Ihrem lokalen Netz erhalten die IP-Adressen direkt vom DHCP-Server des Kabelnetzbetreibers.




*In diesem Beispiel ist nur ein Rechner über das ELSA MicroLink Cable mit dem Internet verbunden. Im Prinzip können aber auch mehrere Rechner, z.B. über einen Hub, an das ELSA MicroLink Cable angeschlossen werden, sofern der Netzbetreiber dies zuläßt.*

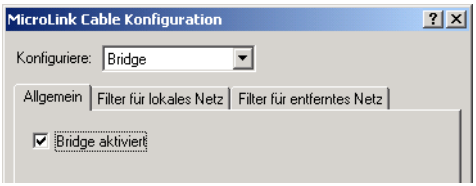
Die Einstellungen können Sie entweder mit dem Setup-Assistenten oder direkt in der Konfiguration vornehmen.

DE

① Starten Sie *ELSA LANconfig* mit **Start** ▶ **Programme** ▶ **ELSAlan** ▶ ***ELSA LANconfig***.

② Klicken Sie auf den Eintrag für das *ELSA MicroLink Cable* in der Geräteliste, um den Konfigurationsdialog zu öffnen. Falls noch kein Eintrag vorhanden ist, wählen Sie **Gerät** ▶ **Suchen**. *ELSA LANconfig* findet alle vorhandenen Geräte und zeigt sie im Listenfenster an.

③ Wechseln Sie in den Konfigurationsbereich 'Bridge' und aktivieren Sie auf der Registerkarte 'Allgemein' die 'Bridge'.




④ Wechseln Sie dann in den Konfigurationsbereich 'TCP/IP' und deaktivieren Sie auf der Registerkarte 'Router' die Option 'IP-Router'. Deaktivieren Sie außerdem auf der Registerkarte 'DHCP-Server' den DHCP-Server in Ihrem *ELSA MicroLink Cable* sowie die Funktion 'IP-Masquerading' auf der Registerkarte 'Masquerading'.

⑤ Speichern Sie die Änderungen in der Konfiguration mit **OK**.

Damit ist das *ELSA MicroLink Cable* fertig eingestellt für die Betriebsart als Bridge. Starten Sie Ihren Web-Browser und los geht's ins WWW mit bisher nicht gekannter Geschwindigkeit ...

*Falls Sie nach dieser Konfiguration nur mit einem Rechner auf das Internet zugreifen können, die anderen Rechner aber keinen Kontakt zum WWW bekommen, hat Ihr Kabelnetzbetreiber evtl. die maximale Anzahl der angeschlossenen Rechner eingeschränkt. Das Kabelmodem überträgt dann nur die Datenpakete der Rechner, die es zuerst bis zu der maximal erlaubten Anzahl von Rechnern erkannt hat. Die Daten aller weiteren Rechner werden nicht übertragen. Bitten Sie in diesem Fall entweder den Netzbetreiber, diese Anzahl zu erhöhen, oder konfigurieren Sie Ihr ELSA MicroLink Cable als Router (mit DHCP-Server und IP-Masquerading).*

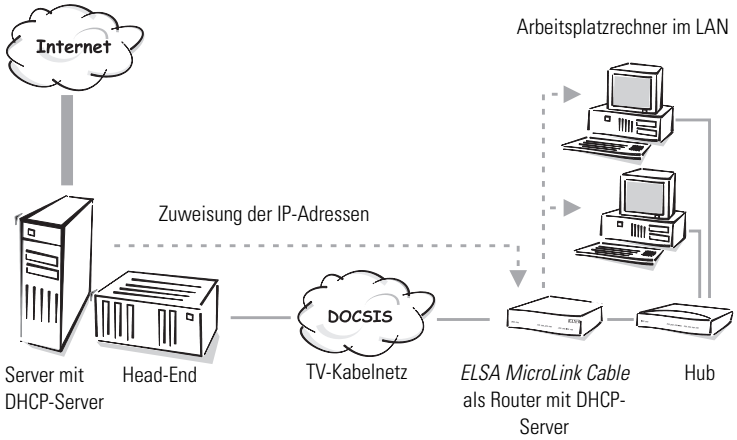
*Um den Austausch von Datenpaketen mit dem Internet einzuschränken, können Sie für das lokale Netz und das Internet geeignete Filter definieren.*

DE

## 3.4 Konfiguration als Router

*Mit ELSA LANconfig rufen Sie einfach den entsprechenden Setup-Assistenten im Menü 'Extras' auf. Er ermöglicht eine schnelle und komfortable Konfiguration des Kabelmodems. In diesem Abschnitt beschreiben wir die „manuelle Methode" Schritt für Schritt.*

Neben der Betriebsart als Bridge kann das *ELSA MicroLink Cable* auch als IP-Router seine Dienste verrichten. Bei dieser Arbeitsweise achtet das *ELSA MicroLink Cable* sehr wohl auf die IP-Adressen der Rechner, die Daten mit dem Internet austauschen wollen. Daher läßt sich in dieser Betriebsart der Datenaustausch mit dem Internet wesentlich genauer einstellen. Die Verwendung der Funktionen DHCP-Server und IP-Masquerading helfen Ihnen bei der Verwaltung der IP-Adressen im LAN.




*In diesem Beispiel sind mehrere Rechner über einen Hub an das ELSA MicroLink Cable angeschlossen und so mit dem Internet verbunden. Im Prinzip kann aber auch ein einzelner Rechner direkt an das ELSA MicroLink Cable angeschlossen werden.*

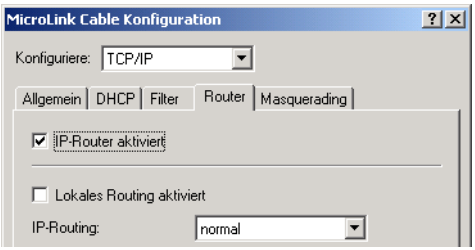
① Starten Sie *ELSA LANconfig* mit **Start** ▶ **Programme** ▶ **ELSAlan** ▶ ***ELSA LANconfig***.

② Damit ein Gerät den anderen Geräten in einem TCP/IP-Netz Adressen zuweisen kann, braucht es zunächst einmal selbst eine im LAN gültige IP-Adresse (LAN-IP-Adresse). Klicken Sie auf den Eintrag in der Geräteliste,

um den Konfigurationsdialog zu öffnen. Falls noch kein Eintrag vorhanden ist, können Sie mit **Gerät ▶ Suchen** automatisch nach Geräten suchen. Oder Sie legen mit **Gerät ▶ Neu** einen neuen Eintrag in der Geräteliste an. Geben Sie dabei als IP-Adresse '10.0.0.254' oder 'x.x.x.254' ein, wobei 'x.x.x' für den evtl. bisher im Netz verwendeten Adreßkreis steht. Wechseln Sie in den Konfigurationsbereich 'TCP/IP' und tragen Sie auf der Registerkarte 'Allgemein' die LAN-IP-Adresse mit der zugehörigen Netzmaske ein.

- Wenn Sie bisher noch keine IP-Adressen in Ihrem Netz verwendet haben, dann geben Sie dem Gerät eine beliebige Adresse aus einem der für private Zwecke reservierten Adreßbereiche, z.B. '10.0.0.1' mit der Netzmaske '255.255.255.0'. Damit legen Sie auch gleichzeitig den Adreßbereich fest, den der DHCP-Server anschließend für die anderen Geräte im Netz verwendet.
- Falls Sie bisher schon IP-Adressen auf den Rechnern im LAN eingestellt hatten, geben Sie dem Gerät eine freie Adresse aus dem bisher verwendeten Adreßbereich.
- Beachten Sie in jedem Fall, daß Sie LAN-seitig nur ein Netzwerk konfigurieren, das vom TV-Kabelnetz verschieden ist.

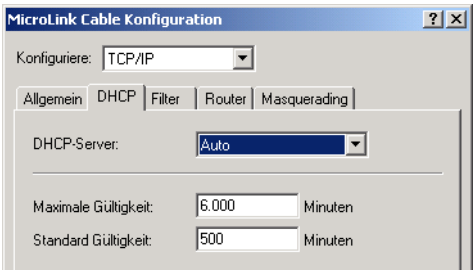
③ Wählen Sie nun auf der Registerkarte 'Router' die Option 'IP-Router aktiviert'.




④ Aktivieren Sie auf der Registerkarte 'Masquerading' die Funktion 'IP-Masquerading'. Dadurch werden die in Ihrem lokalen Netz verwendeten IP-Adressen nicht im Internet sichtbar. Dieses Verhalten sichert zum einen Ihr Netz gegen ungewünschte Eingriffe ab und vermeidet zum anderen Konflikte mit anderen Netzwerken, die evtl. intern die gleichen Adressen verwenden (siehe auch IP-Adressierung und IP-Masquerading).

⑤ Wechseln Sie auf die Registerkarte 'DHCP' und stellen Sie den DHCP-Server auf den Automodus ein. Damit kann das Gerät die IP-Adressen im

lokalen Netz selbständig verwalten. Den gültigen Adreßpool berechnet das *ELSA MicroLink Cable* selbst aus der eigenen LAN-IP-Adresse, sofern Sie nichts anderes bestimmen.




⑥ Wechseln Sie dann in den Konfigurationsbereich 'Bridge' und deaktivieren Sie auf der Registerkarte 'Allgemein' die Option 'Bridge'.

⑦ Speichern Sie die Änderungen in der Konfiguration mit **OK**.

Damit ist das *ELSA MicroLink Cable* fertig eingestellt für die Betriebsart als Router. Starten Sie Ihren Web-Browser und los geht's ins WWW mit bisher nicht gekannter Geschwindigkeit ...

*Um den Austausch von Datenpaketen mit dem Internet einzuschränken, können Sie für das lokale Netz und das Internet geeignete Filter definieren. Damit können Sie z.B. einschränken, welcher Rechner überhaupt auf das Internet zugreifen darf oder welche Seiten im WWW nicht abgefragt werden dürfen.*

## 3.5 Was ist los auf der Leitung?

### 3.5.1 Trace-Ausgaben

Zur Kontrolle der internen Abläufe im Kabelmodem während oder nach der Konfiguration bieten sich die Trace-Ausgaben an. Die Trace-Ausgaben stehen Ihnen unter Telnet zur Verfügung.

*Die Trace-Ausgaben sind leicht zeitverzögert zum tatsächlichen Ereignis, jedoch immer in der richtigen Reihenfolge. Das stört im Regelfall die Interpretation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.*

DE

### So starten Sie einen Trace

Der Trace-Aufruf folgt dieser Syntax:

```
trace [Schlüssel] [Parameter]
```

Der Befehl Trace, der Schlüssel, die Parameter und die Kombinationsbefehle werden jeweils durch Leerzeichen voneinander getrennt. Und was steckt hinter Schlüssel und Parameter?

| Dieser Schlüssel ... | ... ruft in Verbindung mit Trace die folgende Reaktion hervor: |
|---|---|
| ? | zeigt einen Hilfetext an |
| + | schaltet eine Trace-Ausgabe ein |
| - | schaltet eine Trace-Ausgabe aus |
| # | schaltet zwischen verschiedenen Trace-Ausgaben um (Toggle) |
| kein Schlüssel | zeigt den aktuellen Zustand des Traces an |

| Dieser Parameter ... | ... ruft beim Trace die folgende Anzeige hervor: |
|---|---|
| Status | Status-Meldungen der Verbindungen |
| Error | Fehler-Meldungen der Verbindungen |
| IP-Router | IP-Routing |
| IP-RIP | IP Routing Information Protocol |
| ICMP | Internet Control Message Protocol |
| ARP | Address Resolution Protocol |
| IP-Masquerading | Vorgänge im Masquerading-Modul |
| DHCP | Dynamic Host Configuration Protocol |

| Dieser Kombinations-Befehl ... | ... ruft beim Trace die folgende Anzeige hervor: |
|---|---|
| All | alle Trace-Ausgaben |
| Display | Status- und Error-Ausgaben |
| TCP-IP | IP-Rt.-, IP-RIP-, ICMP- und ARP-Ausgaben |
| Time | zeigt vor der eigentlichen Trace-Ausgabe auch die Systemzeit an |
| Source | zeigt vor der eigentlichen Trace-Ausgabe auch das Protokoll an, das die Ausgabe veranlaßt hat |

Die angehängten Parameter werden dabei von links nach rechts abgearbeitet. Dadurch kann ein zunächst aufgerufener Parameter anschließend auch wieder eingeschränkt werden.

**Beispiele:**

| Dieser Schlüssel ... | ... ruft in Verbindung mit Trace die folgende Reaktion hervor: |
|---|---|
| trace | zeigt alle Protokolle an, die während der Konfiguration Ausgaben erzeugen können, und den Zustand der jeweiligen Ausgaben (ON oder OFF). |
| trace + all | schaltet alle Trace-Ausgaben ein. |
| trace + all - icmp | schaltet alle Trace-Ausgaben mit Ausnahme des ICMP-Protokolls ein. |
| trace - time | schaltet die Ausgabe der Systemzeit vor der eigentlichen Trace-Ausgabe ab. |

*Hinweise zur Interpretation der Trace-Ausgaben finden Sie im Referenz-Teil des Handbuchs.*

## 3.6 Neue Firmware mit FirmSafe

Die Software der Geräte von ELSA wird ständig weiterentwickelt. Damit Sie auch in den Genuß von neuen Features und Funktionen kommen, haben wir die Geräte mit einem Flash-ROM-Speicher ausgerüstet, der das nachträgliche Ändern der Betriebssoftware zum Kinderspiel macht. Kein EPROM tauschen, kein Gehäuse öffnen: Einfach die neue Version einspielen und fertig!

*Im Normalfall sorgt Ihr Provider für die Aktualisierung der Firmware und den Upload. Von Ihnen eingespielte Firmware-Versionen können dadurch überschrieben werden.*

### 3.6.1 So funktioniert FirmSafe

FirmSafe macht das Einspielen der neuen Software zur sicheren Sache: Die gerade verwendete Firmware wird dabei nicht einfach überschrieben, sondern es wird eine zweite Firmware zusätzlich im Gerät gespeichert.

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firm-

ware überschrieben. Sie können selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll:

- 'Unmittelbar': Als erste Möglichkeit können Sie die neue Firmware laden und sofort aktivieren. Folgende Situationen können dann entstehen:
  - Die neue Firmware wird erfolgreich geladen und arbeitet anschließend wie gewünscht. Dann ist alles in Ordnung.
  - Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Falls schon während des Uploads ein Fehler auftritt, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Login': Um den Problemen eines fehlerhaften Uploads zu begegnen, gibt es die zweite Möglichkeit, bei der die Firmware geladen und ebenfalls sofort gestartet wird.
  - Im Unterschied zur ersten Variante wartet das Gerät anschließend fünf Minuten lang auf einen erfolgreichen Login per Telnet. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.
  - Wenn das Gerät nicht mehr ansprechbar ist und ein Login somit unmöglich ist, aktiviert das Gerät automatisch wieder die bisherige Firmware und startet damit das Gerät neu.
- 'Manuell': Bei der dritten Möglichkeit können Sie vorher selbst eine Zeit bestimmten, in der Sie die neue Firmware testen wollen. Das Gerät startet mit der neuen Firmware und wartet in der eingestellten Zeit darauf, daß die geladene Firmware von Hand aktiviert und damit dauerhaft wirksam gemacht wird.

### 3.6.2 So spielen Sie eine neue Software ein

Beim Firmware-Upload (so heißt das Einspielen der Software) gibt es verschiedene Wege zum Ziel:

- *ELSA LANconfig* (empfohlen)
- TFTP

Beim Firmware-Upload bleiben alle Einstellungen erhalten! Trotzdem sollten Sie sicherheitshalber die Konfiguration vorher speichern (bei ***ELSA LANconfig*** z.B. mit **Bearbeiten ▶ Konfiguration sichern**).

Enthält die neu eingespielte Version Parameter, die in der aktuellen Firmware des Gerätes nicht vorhanden sind, werden die fehlenden Werte mit den Default-Einstellungen ergänzt.

DE

### *ELSA LANconfig*

In *ELSA LANconfig* markieren Sie das gewünschte Gerät in der Auswahlliste und klicken auf **Bearbeiten ▶ Firmware-Verwaltung ▶ Neue Firmware hochladen** oder direkt auf die Schaltfläche **Firmware-Upload**. Dann wählen Sie das Verzeichnis, in dem sich die neue Version befindet, und markieren die entsprechende Datei.

*ELSA LANconfig* informiert Sie dann in der Beschreibung über Versions-Nr. und Datum der Firmware und bietet den Upload an. Mit **Öffnen** ersetzen Sie die vorhandene Firmware durch die ausgewählte Version.

Wählen Sie außerdem aus, ob die Firmware sofort nach dem Laden dauerhaft aktiviert werden soll, oder stellen Sie eine Testzeit ein, in der Sie die Firmware selbst freischalten. Um anschließend die Firmware während der eingestellten Testzeit zu aktivieren, klicken Sie auf **Bearbeiten ▶ Firmware-Verwaltung ▶ Firmware im Test freischalten**.

### TFTP

Über TFTP kann eine neue Firmware mit dem Befehl **writeflash** eingespielt werden. Um eine neue Firmware, die z.B. in der Datei 'CM_110F.UPX' vorliegt, in ein Gerät mit der IP-Adresse 194.162.200.17 zu übertragen, geben Sie z.B. unter Windows NT folgenden Befehl ein:

```
tftp -i 194.162.200.17 put CM_110F.UPX
writeflash
```

*Durch diesen Befehl wird die entsprechende Datei mit dem Kommando **writeflash** an das Gerät gesendet. Dabei muß für TFTP die binäre Dateiübertragung eingestellt werden. Auf vielen Systemen ist jedoch das ASCII-Format voreingestellt. In diesem Beispiel für Windows NT erreichen Sie das durch den Parameter '-i'.*

Nach einem erfolgreichen Firmware-Upload bootet das Gerät und aktiviert so direkt die neue Firmware. Tritt während des Uploads ein Fehler auf (Schreibfehler im Flash-ROM, TFTP-Übertragungsfehler o.ä.) so wird die TFTP-Verbindung abgebrochen, um dem Anwender einen Hinweis auf ein Problem zu liefern. Das Gerät bootet in diesem Fall nicht, sondern arbeitet bis zum nächsten Aus- und Einschalten mit der bisherigen Firmware weiter. Der Anwender erhält so die Möglichkeit, die aktuelle Konfiguration des Gerätes zu retten.

Mit TFTP können auch andere Konfigurations-Befehle ausgeführt werden. Die Syntax ist am einfachsten den folgenden Beispielen zu entnehmen:

DE

- `tftp 10.0.0.1 get readconfig file1`
  Liest die Konfiguration aus dem Gerät mit der Adresse 10.0.0.1 und speichert diese unter file1 im aktuellen Verzeichnis ab
- `tftp 10.0.0.1 put file1 writeconfig`
  Schreibt die Konfiguration aus file1 in das Gerät mit der Adresse 10.0.0.1
- `tftp 10.0.0.1 get dir/status/tcp-ip-statistik file2`
  Speichert die aktuellen TCP-IP-Statistik in file2

## 3.7 Konfiguration über SNMP

In diesem Abschnitt wird die Konfiguration über SNMP beschrieben. Beachten Sie, daß je nach Netzwerkbetreiber der SNMP-Zugriff über das LAN eingeschränkt sein kann. So ist es möglich, daß Sie auf Ihr Kabelmodem über SNMP nur lesend (GetRequest, GetNextRequest und GetBulkRequest) oder gar nicht zugreifen können.

### 3.7.1 Allgemeines

Das **S**imple **N**etwork **M**anagement **P**rotocol (SNMP) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus. Diese Instanz wird im üblichen Sprachgebrauch „Manager" genannt, während die Geräte „Agents" genannt werden. Die erlaubte Struktur des SNMP-Informationsaustauschs ist relativ simpel. Eine Manager-Applikation hat im Netz Zugriff auf alle SNMP-fähigen Geräte und Dienste (die Agents). Die Zugriffsberechtigungen werden über „Communities" geregelt.

Die folgende Tabelle zeigt den Befehlssatz des im Gerät implementierten SNMP-Agenten (SNMPv1 und SNMPv2c):

| Befehl | Ziel/Quelle | Funktion |
|---|---|---|
| GetRequest | Manager – Agent | ruft eine Information vom Agent ab |
| GetNextRequest | Manager – Agent | ruft die in der MIB folgende Information vom Agent ab |
| GetBulkRequest | Manager – Agent | es können mehrere, hintereinanderliegende Objekte ausgelesen werden |
| SetRequest | Manager – Agent | ändert eine Einstellung beim Agent |
| GetResponse | Agent – Manager | liefert den abgefragten Wert an den Manager zurück |

| Befehl | Ziel/Quelle | Funktion |
|---|---|---|
| Trap | Agent – Manager | meldet einen Fehler oder einen besonderen Zustand |

Mit Hilfe dieser Befehle können SNMP-fähige Geräte in einem Netz zentral überwacht und konfiguriert werden. Die SNMP-Fähigkeiten der Agents werden in sogenannten MIBs = Management Information Bases festgelegt.

Unterstützt wird ein Teil der MIB-2 und eine private MIB, die als separate Datei dem Produkt beiliegt. Um einen Gerät vollständig über SNMP verwalten zu können, muß diese MIB von einem SNMP-Manager (z.B. HP-OpenView) geladen und übersetzt werden. Danach stehen alle Menüs und Parameter der Konfiguration in einem eigenen Ast des SNMP-Management-Baums zur Verfügung.

## 3.7.2 Zugriff auf Tabellen und Parameter über SNMP

Fast alle Tabellen und Parameter können über die SNMP-Schnittstelle gelesen und ggf. auch geändert werden. Dabei wird in der MIB festgelegt, welche Variablen den Status 'read-only' oder 'read-write' haben. In handelsüblichen SNMP-Managern sind die beiden Zustände 'read-only' und 'read-write' in der Regel farblich gekennzeichnet.

### Zugriffschutz des SNMP-Agenten

Der Zugriff auf SNMP-Objekte erfolgt über sogenannte Communities. Eine Community ist im Grunde ein Paßwort, mit dem der Zugriff auf bestimmte Informationsklassen gesteuert werden kann. Falls vom Provider keine Zugriffsbeschränkung auferlegt wurde, kann über die Community 'public' gelesen und über 'private' geschrieben werden.

Bei einem fehlgeschlagenen Zugangsversuch wird ein Trap 'Authentication Failed' ausgelöst und an den/die Manager in der SNMP-Trap-Tabelle geschickt, wenn der Trap-Mechanismus eingeschaltet wurde.

Der Community-Mechanismus von SNMPv1 und SNMPv2c ist allerdings nur ein sehr eingeschränkter Zugriffsschutz, da sowohl die Daten, die MIB-IDs als auch die Community innerhalb der Requests und Responses unverschlüsselt im UDP-Datenblock verschickt werden.

#### Tabellen-Zeilen hinzufügen mit SNMP

Das Anlegen von neuen Tabellenzeilen via SNMP geschieht durch Setzen eines neuen Indexeintrages. Mit dem Befehl in der Syntax:

```
someTable.1.2.2 = xyz
```

wird in der Tabelle „someTable" eine Zeile mit dem Index „2" erzeugt, in deren zweiter Spalte der wert „xyz" eingetragen wird. Die „1" hinter dem Tabellennamen ist für diesen Befehl konstant und steht in der SNMP-Syntax für „someEntry".

#### Fehlermeldungen per SNMP-Trap

Über den Mechanismus der SNMP-Traps können Ereignisse an eine Management-Instanz gesendet werden. Dies können z.B. Fehler- oder Warnmeldungen sein. Der SNMP-Agent erlaubt das Versenden von Traps an bis zu 20 SNMP-Manager. Die IP-Adressen dieser Manager werden im Konfigurations-Menü unter `/setup/SNMP-Modul/IP-Trap-Tabelle` konfiguriert. Falls Ihr Provider das Senden von Traps freigeschaltet hat, können Sie das Versenden mit dem Schalter `/setup/snmp-Modul/Send-Traps` ein- und ausschalten.

Das Ein- und Ausschalten von Trap-Empfängern kann auch über *ELSA LANconfig* durchgeführt werden (Management/SNMP).

### 3.7.3 Die Management-Information-Base (MIB)

Um SNMP-Management-Systemen Zugriff auf die Konfiguration im *ELSA MicroLink Cable* zu geben, muß eine textuelle Darstellung der Konfigurationsstruktur (die sogenannte private MIB) vorliegen. Die Syntax dieser MIB orientiert sich an der ASN.1 (Abstract Syntax Notation One, ISO 8824). In der Regel ist im Programmpaket der SNMP-Management-Software ein sogenannter MIB-Compiler enthalten. Dieser Compiler übersetzt die MIB-Datei in eine vom Manager benutzbare Form.

Die aktuelle ELSA-MIB ist sowohl als Beilage zum Produkt auf der CD zu finden, als auch auf den ELSA-Online-Medien.

DE

# 4 Funktionen und Betriebsarten

Dieses Kapitel stellt Ihnen die Funktionen und Betriebsarten Ihres Gerätes vor. Dabei finden Sie u.a. Informationen zu den folgenden Punkten:

- Sicherheit für die Konfiguration
- Sicherheit für das LAN
- IP-Routing
- Bridging
- DHCP-Server

Neben der Beschreibung der einzelnen Punkte geben wir Ihnen hier auch Hinweise, die Sie bei der Konfiguration unterstützen.

Ausführliche Konfigurationsbeispiele finden Sie im Kapitel 'Konfigurationsmöglichkeiten' ab Seite 25.

Eine detaillierte Beschreibung aller Parameter und Menüs finden Sie in der elektronischen Dokumentation.

## 4.1 Sicherheit für Ihre Konfiguration

Mit der Konfiguration des Gerätes legen Sie eine Reihe von wichtigen Parametern für den Datenaustausch fest: Die Sicherheit des eigenen Netzes, die Kontrolle der Kosten und die Berechtigung einzelner Netzteilnehmer gehören z.B. dazu.

Die von Ihnen einmal eingestellten Parameter sollen natürlich nicht durch Unbefugte verändert werden. Daher bietet ein *ELSA MicroLink Cable* die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

### 4.1.1 Paßwortschutz

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Paßworts. Solange Sie kein Paßwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern.

Das Feld zur Eingabe des Paßworts finden Sie in *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Bei einer Terminal- oder Telnetsitzung schalten Sie die Paßwortabfrage im Menü `/Setup/Config-Modul/Passw.Zwang` ein. Das Paßwort selbst wird in diesem Fall mit dem Befehl `passwd` gesetzt.

DE

### 4.1.2 Die Login-Sperre

Die Konfiguration im *ELSA MicroLink Cable* ist durch eine Login-Sperre gegen „Brute-Force-Angriffe" geschützt. Bei einem Brute-Force-Angriff versucht ein unberechtigter Benutzer ein Paßwort zu „knacken", und so Zugang zu einem Netzwerk, einem Rechner oder einem anderen Gerät zu erlangen. Dazu spielt z.B. ein Rechner automatisch alle möglichen Kombinationen aus Buchstaben und Zahlen durch, bis das richtige Paßwort gefunden wurde.

Zum Schutz gegen solche Versuche kann die maximal zulässige Anzahl von fehlerhaften Login-Versuchen eingegeben werden. Wird dieser Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt.

Diese Parameter gelten global für alle Konfigurationsmöglichkeiten (Telnet, TFTP/*ELSA LANconfig* und SNMP). Tritt auf einem Zugang die Sperre in Kraft, so sind auch alle anderen Zugänge automatisch gesperrt.

Zur Konfiguration der Login-Sperre stehen in *ELSA LANconfig* im Konfigurationsbereich 'Management' auf der Registerkarte 'Security' bzw. im Menü `/Setup/Config-Modul` die folgenden Einträge zur Verfügung:

- 'Sperre aktivieren nach' (`Login-Fehler`)
- 'Dauer der Sperre' (`Sperr-Minuten`)

### 4.1.3 Zugangskontrolle über TCP/IP

Mit einer speziellen Filterliste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfigurationssitzungen über Telnet oder TFTP (*ELSA LANconfig*) bezeichnet.

Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf das Gerät gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen.

Die Zugangsliste finden Sie in *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein' bzw. im Menü `/Setup/TCP-IP-Modul/Zugangsliste`.

DE

## 4.2 Sicherheit für Ihr LAN

Sie mögen es sicher nicht, wenn jeder Außenstehende einfach die Daten auf Ihren Rechnern einsehen oder verändern kann. Ein *ELSA MicroLink Cable* bietet verschiedene Möglichkeiten, den Zugriff von außen einzuschränken:

- Verschlüsselung des Datenstroms
- Filterung von Datenpaketen
- IP-Masquerading (auch NAT oder PAT genannt)

### 4.2.1 Verschlüsselung

Da Kabelmodems die Daten über ein Kabel übertragen, das viele Teilnehmer gemeinsam nutzen, müssen die Daten für andere Teilnehmer unbrauchbar, also verschlüsselt werden.

Alle Daten zwischen dem Modem des Providers und dem Modem des Endanwenders werden automatisch verschlüsselt übertragen. Hierbei kommt die DES-Verschlüsselung (Data Encription Standard) mit einer Schlüssellänge von 56 bit zum Einsatz. Zusätzlich wird der verwendete Schlüssel während der Datenübertragung wiederholt gewechselt. Dadurch werden auch höchste Sicherheitsanforderungen erfüllt.

### 4.2.2 Filter für die TCP/IP-Pakete

Mit den Einträgen in der Routing-Tabelle können Sie schon recht genau festlegen, welche Datenpakete übertragen werden sollen. Zusätzlich können Sie mit dem Eintrag '0.0.0.0' im Feld 'Router-Name' ganze Gruppen von IP-Adressen verwerfen.

Manchmal möchten Sie die Übertragung jedoch noch weiter einschränken. Dazu nutzen Sie die Eigenschaft von TCP/IP, neben den Quell- und Ziel-IP-Adressen mit einem Datenpaket auch Portnummern für Ziel und Quelle zu versenden. Der Ziel-Port in einem Datenpaket steht für den Dienst im TCP/IP-Netz, der angesprochen werden soll. Die Ziel-Ports für verschiedene Dienste im TCP/IP-Netz sind fest definiert (siehe auch 'TCP/IP-Ports' Referenz-Handbuch). Die Quell-Ports hingegen werden in bestimmten Bereichen frei gewählt.

Das Gerät kann sich die Ziel- und Quell-Ports von solchen Datenpaketen ansehen, die TCP oder UDP als Protokoll verwenden. Aus diesen Ports kann dann abgeleitet werden, für welchen Zweck die Daten gedacht sind. So können z.B. FTP-Zugriffe oder Telnet-Sitzungen erkannt werden.

Mit Hilfe der entsprechenden Filter-Tabelle können Sie festlegen, daß bestimmte Daten nicht aus dem LAN an das Kabelnetz übertragen werden sollen. Genauso können natürlich auch Daten für bestimmte Ports aus dem Kabelnetz in Richtung des LANs gesperrt werden.

Neben der Definition der Portbereiche und der zugehörigen Protokolle kann in den Filter-Tabellen mit dem Filter-Typ auch festgelegt werden, ob die betroffenen Datenpakete nie übertragen werden oder ob sie nur nicht zu einem Verbindungsaufbau führen sollen (also nur bei bestehender Verbindung übertragen werden).

Diese Filtertabellen finden Sie in *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Filter' bzw. im Menü `/Setup/IP-Router-Modul`.

### 4.2.3 Das Versteck – IP-Masquerading (NAT, PAT)

Eine der häufigsten Aufgaben für ein Kabelmodem ist heute die Anbindung vieler Arbeitsplätze in einem LAN an das Netz der Netze, das Internet. Jeder soll nach Möglichkeit direkt von seinem Arbeitsplatz aus auf das WWW zugreifen und sich brandaktuelle Informationen für seine Arbeit holen können.

Aber da gibt es Einwände der Netzwerkbetreuer, die sich um die Sicherheit der Daten im firmeneigenen Netz sorgen: Jeder Arbeitsplatzrechner im WWW? Da kann doch dann auch jeder von außen dran! – Kann er nicht!

IP-Masquerading heißt das Versteck für alle Rechner im Internet. Dabei wird nur das Routermodul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt dabei Internet und Intranet wie eine Wand. IP-Masquerading wird daher auch als „Firewall-Technik" bezeichnet.

Weitere Informationen finden Sie im Abschnitt 'IP-Routing: IP-Masquerading'.

## 4.3 IP-Routing

*In diesem Kapitel wird die Funktion des Kabelmodems als IP-Router beschrieben. Wenn in den folgenden Abschnitten von IP-Router (oder einfach nur Router) die Rede ist, ist damit die entsprechende Betriebsart des Kabelmodems gemeint.*

Ein IP-Router arbeitet zwischen Netzen, die TCP/IP als Netzwerk-Protokoll verwenden. Dabei werden nur Daten übertragen, deren Zieladressen in der Routing-Tabelle eingetragen sind. In diesem Kapitel erfahren Sie, wie die IP-Routing-Tabelle in einem Router von ELSA aufgebaut ist und mit welchen weiteren Funktionen das IP-Routing unterstützt wird.

### 4.3.1 Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welchen anderen Router oder Rechner er die Daten für bestimmte IP-Adressen oder IP-Adreß-Bereiche schicken soll. So ein Eintrag heißt auch „Route", weil der Weg der Datenpakete damit beschrieben wird. Da Sie diese Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing". Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing". Dabei tauschen mehrere Router selbständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Die statische Routing-Tabelle kann bis zu 64 Einträge aufnehmen, die dynamische Tabelle 128. Bei aktiviertem IP-RIP beachtet der IP-Router beide Tabellen.

Die Routingtabelle finden Sie in *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' bzw. im Menü `/Setup/IP-Router/IP-Routing-Tab`. So sieht eine IP-Routing-Tabelle also z.B. aus:

| IP-Adresse | IP-Netzmaske | Router | Distanz |
|---|---|---|---|
| 192.168.0.0 | 255.255.0.0 | 0.0.0.0 | 0 |
| 172.16.0.0 | 255.255.0.0 | 0.0.0.0 | 0 |
| 10.0.0.0 | 255.0.0.0 | 0.0.0.0 | 0 |
| 224.0.0.0 | 224.0.0.0 | 0.0.0.0 | 0 |
| 255.255.255.255 | 0.0.0.0 | CABLE | 1 |
| 192.168.130.0 | 255.255.255.0 | 191.168.140.123 | 1 |

Was bedeuten die einzelnen Einträge in der Liste?

- IP-Adresse und IP-Netzmaske

  Das ist die Adresse des Zielnetzes, zu dem Datenpakete geschickt werden können, mit der zugehörigen Netzmaske. Mit der Netzmaske und der

Ziel-IP-Adresse aus den ankommenden Datenpaketen prüft der Router, ob das Paket in das Zielnetz gehört.

Die Route mit der IP-Adresse „255.255.255.255" mit Netzmaske „0.0.0.0" ist die Default-Route. Alle Datenpakete, die nicht durch andere Routing-Einträge geroutet werden können, werden über diese Route übertragen.

- Router-Name

  Der Router-Name gibt an, was mit den zur IP-Adresse und Netzmaske passenden Datenpaketen geschehen soll.

  Routen mit dem Router-Name „0.0.0.0" bezeichnen Ausschluß-Routen. Datenpakete für diese „Null-Routen" werden verworfen und nicht weitergeleitet. Damit werden z.B. die im Internet verbotenen Routen (Privat Address Spaces, z.B. 10.0.0.0) von der Übertragung ausgeschlossen.

  Wird als Router-Name eine IP-Adresse eingetragen, handelt es sich dabei um einen lokal erreichbaren Router, der für die Übertragung der entsprechenden Datenpakete zuständig ist.

  Im Kabelmodem finden Sie standardmäßig bei der Default-Route den Eintrag „CABLE" als Router-Name. Alle IP-Datenpakete, die über diese Route übertragen werden, werden zum Kabelinterface geleitet.

- Distanz

  Anzahl der zwischen dem eigenen und dem Ziel liegenden Router.

  Beispiele mit Erläuterungen:

| IP-Adresse | IP-Netzmaske | Router-Name | Dist. | Und das passiert: |
|---|---|---|---|---|
| 192.168.130.0 | 255.255.255.0 | 192.168.140.123 | 0 | Alle Datenpakete mit den Ziel-IP-Adressen 192.168.130.x werden an den lokal erreichbaren Router mit der IP-Adresse 192.168.140.123 übertragen. |
| 192.168.0.0 | 255.255.0.0 | 0.0.0.0 | 0 | Schließt die Übertragung aller Datenpakete in Netzwerke aus, die sich nicht im Internet befinden dürfen. |
| 172.16.0.0 | 255.255.0.0 | 0.0.0.0 | 0 | |
| 10.0.0.0 | 255.0.0.0 | 0.0.0.0 | 0 | |
| 224.0.0.0 | 224.0.0.0 | 0.0.0.0 | 0 | |
| 255.255.255.255 | 0.0.0.0 | CABLE | 1 | Alle Datenpakete, die nicht den zuvorstehenden Einträgen zugeordnet werden können, werden in das Kabelnetz übertragen. |

DE

## 4.3.2 Dynamisches Routing mit IP-RIP

Neben der statischen Routing-Tabelle verfügen Router von ELSA auch über eine dynamische Routing-Tabelle mit bis zu 128 Einträgen. Diese Tabelle füllt der Anwender im Gegensatz zu der statischen nicht selbst aus, das erledigt der Router selbst. Dazu nutzt er das Routing Information Protocol (RIP). Über dieses Protokoll tauschen alle Geräte, die RIP beherrschen, Informationen über die erreichbaren Routen aus.

### Welche Informationen werden über IP-RIP propagiert?

Ein Router teilt in den IP-RIP-Informationen den anderen Routern im Netz die Routen mit, die es in seiner eigenen statischen Tabelle findet. Nicht berücksichtigt werden dabei die folgenden Einträge:

- Routen, die mit der Router-Einstellung '0.0.0.0' verworfen werden
- Routen, die auf andere Router im lokalen Netz lauten

### Welche Informationen nimmt der Router aus empfangenen IP-RIP-Paketen?

Wenn der Router IP-RIP-Pakete empfängt, baut er sie in seine dynamische IP-Routing-Tabelle ein, und die sieht etwa so aus:

| IP-Adresse | IP-Netzmaske | Zeit | Distanz | Router |
|---|---|---|---|---|
| 192.168.120.0 | 255.255.255.0 | 1 | 2 | 192.168.110.1 |
| 192.168.130.0 | 255.255.255.0 | 5 | 3 | 192.168.110.2 |
| 192.168.140.0 | 255.255.255.0 | 1 | 5 | 192.168.110.3 |

### Was bedeuten die Einträge?

IP-Adresse und Netzmaske bezeichnen das Ziel-Netz, die Distanz gibt die Anzahl der zwischen Sender und Empfänger liegenden Router an, die letzte Spalte zeigt an, welcher Router diese Route bekanntgemacht hat. Bleibt die 'Zeit'. Damit zeigt die dynamische Tabelle an, wie alt die entsprechende Route ist. Der Wert in dieser Spalte gilt als Multiplikator für das Intervall, in dem die RIP-Pakete eintreffen, eine '1' steht also für etwa 30 Sekunden, eine '5' für etwa 2,5 Minuten usw. Wenn eine Information über eine Route neu eintrifft, gilt diese Route natürlich als direkt erreichbar und erhält die Zeit '1'. Nach Ablauf der entsprechenden Zeit wird der Wert in dieser Spalte automa-

tisch erhöht. Nach 3,5 Minuten wird die Distanz auf '16' gesetzt (Route nicht erreichbar), nach 5,5 Minuten wird die Route gelöscht.

Wenn der Router nun ein IP-RIP-Paket empfängt, muß er entscheiden, ob er die darin enthaltenen Routen in seine dynamische Tabelle aufnehmen soll oder nicht. Dazu geht er wie folgt vor:

- Die Route ist in der Tabelle noch gar nicht vorhanden, dann wird sie aufgenommen (sofern Platz in der Tabelle ist).
- Die Route ist in der Tabelle vorhanden mit der Zeit von '5' oder '6'. Die neue Route wird dann verwendet, wenn sie die gleiche oder eine bessere Distanz aufweist.
- Die Route ist in der Tabelle vorhanden mit der Zeit von '7' bis '10', hat also die Distanz '16'. Die neue Route wird auf jeden Fall verwendet.
- Die Route ist in der Tabelle vorhanden. Die neue Route kommt von dem gleichen Router, der auch diese Route bekanntgegeben hat, hat aber eine schlechtere Distanz als der bisherige Eintrag. Wenn ein Gerät so die Verschlechterung seiner eigenen statischen Routing-Tabelle bekanntmacht, dann glaubt das Kabelmodem ihm das und nimmt den schlechteren Eintrag in seine dynamische Tabelle auf.

**Zusammenspiel: statische und dynamische Tabelle**

Aus der statischen und der dynamischen Tabelle stellt der Router die eigentliche IP-Routing-Tabelle zusammen, mit der er den Weg für die Datenpakete bestimmt. Dabei nimmt er zu den Routen aus der eigenen statischen Tabelle die Routen aus der dynamischen Tabelle auf, die er selber nicht kennt oder die eine kürzere Distanz aufweisen als die eigene (statische) Route.

### 4.3.3 Lokales Routing

Sie kennen das folgende Verhalten der Arbeitsplatzrechner in einem lokalen Netz: Möchte der Rechner ein Datenpaket an eine IP-Adresse senden, die nicht in seinem eigenen LAN liegt, sucht er nach einem Router, der ihm weiterhelfen kann. Dieser Router wird normalerweise dem Betriebssystem durch den Eintrag als Standard-Router oder Gateway bekanntgegeben. Gibt es in einem Netz mehrere Router, so kann oft nur ein Standard-Router eingetragen werden, der alle dem Arbeitsplatzrechner unbekannten IP-Adressen erreichen können soll. Manchmal kann dieser Standard-Router jedoch nicht selbst das Zielnetz erreichen, er kennt aber einen anderen Router, der zu diesem Ziel findet.

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

Standardmäßig schickt der Router dem Rechner eine Antwort mit der Adresse des Routers, der die Route ins Ziel-Netz kennt (diese Antwort nennt man ICMP-Redirect). Der Arbeitsplatzrechner übernimmt daraufhin diese Adresse und schickt das Datenpaket sofort an den anderen Router.

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing (im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router' oder im Menü `/Setup/IP-Router-Modul/Lok.-Routing Ein`). Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem werden dann keinen ICMP-Redirects mehr geschickt.

Ist im Prinzip ja eine tolle Sache, trotzdem sollte das lokale Routing nur im „Notfall" verwendet werden, denn diese Funktion führt zu einer Verdoppelung aller Datenpakete zum gewünschten Zielnetz. Die Daten werden erst zum Standard-Router und von diesem erneut zum eigentlich zuständigen Router im lokalen Netz geschickt.

### 4.3.4 IP-Masquerading (NAT, PAT)

Ein ständig wachsendes Problem des Internets ist die Begrenzung der verfügbaren und allgemein gültigen IP-Adressen. Darüber hinaus ist die Zuweisung von festen IP-Adressen für das Internet durch das Network Information Center (NIC) eine kostspielige Sache. Was liegt also näher, als sich mit mehreren Rechnern eine IP-Adresse zu teilen?

Die Lösung heißt hier IP-Masquerading. Bei diesem Verfahren tritt nur ein Router des LANs mit einer IP-Adresse im Internet in Erscheinung. Diese IP-Adresse wird dem Router z.B. fest vom NIC oder temporär von einem Internet-Provider zugewiesen. Alle anderen Rechner im Netz „verstecken" sich dann hinter dieser einen IP-Adresse. Neben dem angenehmen Spareffekt bildet das IP-Masquerading auch einen sehr effektiven Schutz gegen Zugriffe aus dem Internet auf das lokale Netz.

*Die Funktion des IP-Masquerading ist an die Betriebsart des Kabelmodems als Router gekoppelt. Wenn in den folgenden Abschnitten von Routern die Rede ist, ist damit das Kabelmodem in der betriebsart als IP-Router gemeint.*

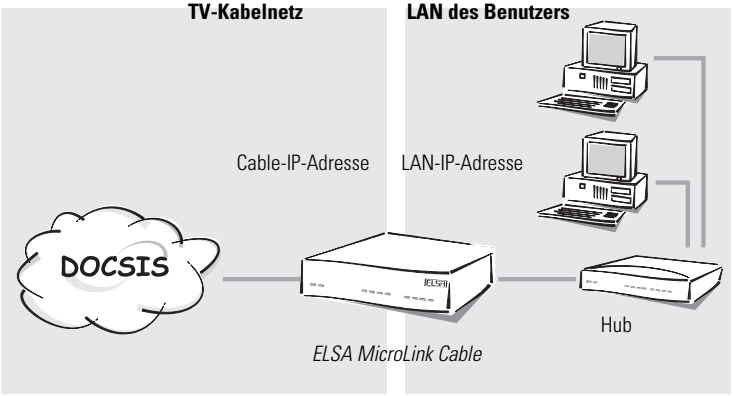
DE

### Zwei Adressen für den Router

Bei Masquerading treffen zwei gegensätzliche Forderungen an den Router aufeinander:

- Zum einen soll er eine im lokalen Netz des Benutzers gültige IP-Adresse haben, damit er aus diesem LAN erreichbar ist.
- Zum anderen soll er eine im Kabelnetz gültige Adresse haben.

Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, hilft hier nur eins: Zwei IP-Adressen müssen her.




Das Kabelmodem bekommt also nun eine Cable-IP-Adresse und eine LAN-IP-Adresse, jeweils natürlich mit passender Netzmaske. Mit der Option 'Masquerading' informieren Sie das Kabelmodem darüber, welche der beiden Adressen es bei der Weitergabe der Pakete verwenden soll.

- 'aus': Es wird keine Maskierung durchgeführt.
- 'ein': Mit diesem Eintrag wird die vom Kabelnetzbetreiber während der Anmeldung am Head-End zugewiesene Cable-IP-Adresse für die Maskierung verwendet.

*Wird das Kabelmodem als IP-Router ohne Masquerading betrieben, muß auf jeden Fall die Verwendung von IP-RIP aktiviert sein! Beim Betrieb als IP-Router mit Masquerading sollte das IP-RIP ausgeschaltet werden.*

### Wie funktioniert IP-Masquerading?

Das Masquerading nutzt die Eigenschaft der Datenübertragung über TCP/IP aus, daß neben der Quell- und Ziel-Adresse auch Portnummer für Quelle und

Ziel verwendet werden. Bekommt der Router nun ein Datenpaket zur Übertragung, merkt er sich die IP-Adresse und den Port des Absenders in einer internen Tabelle. Dann gibt er dem Paket seine eigene Cable-IP-Adresse und eine beliebige neue Portnummer. Diesen neuen Port trägt es ebenfalls in der Tabelle ein und leitet das Paket mit den neuen Angaben weiter.

Die Antwort auf dieses Paket geht nun an die Cable-IP-Adresse des Kabelmodems mit der neuen Absender-Portnummer. Mit dem Eintrag in der internen Tabelle kann der Router diese Antwort nun wieder dem ursprünglichen Absender zuordnen.

*In den Statistiken des Routers können Sie sich diese Tabellen genau ansehen (siehe auch im Referenzhandbuch auf CD).*

### Einfaches und inverses Masquerading

Diese Maskierung funktioniert in beide Richtungen: Wenn ein Rechner aus dem LAN des Benutzers ein Paket ins Internet schickt, wird das lokale Netz hinter der Cable-IP-Adresse des Routers maskiert (einfaches Masquerading).

Schickt umgekehrt ein Rechner aus dem Internet ein Paket z.B. an einen FTP-Server im LAN, so sieht es für diesen Rechner so aus, als wäre der Router der FTP-Server. Der Router liest aus dem Eintrag in der Service-Tabelle die IP-Adresse des FTP-Servers im LAN (im *ELSA LANconfig* im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Masq.' oder im Menü `Setup/IP-Router-Modul/Masquerading/Service-Tabelle`). Das Paket wird an diesen Rechner weitergeleitet. Alle Pakete, die vom FTP-Server im LAN kommen (Antworten des Servers), werden hinter der IP-Adresse des Routers versteckt.

Der kleine Unterschied:

- Der Zugriff von außen auf einen Dienst (Port) im LAN des Benutzers muß vorher durch Angabe einer Port-Nummer definiert werden. In einer Service-Tabelle wird dazu der Ziel-Port mit der LAN-seitigen IP-Adresse z.B. des FTP-Servers angegeben.

- Beim Zugriff aus dem LAN auf das Internet hingegen wird der Eintrag in der Tabelle mit Port- und IP-Adreß-Informationen durch den Router selbst vorgenommen.

  Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also **gleichzeitig** 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

  Nach einer einstellbaren Zeit geht der Router jedoch davon aus, daß der Eintrag nicht mehr benötigt wird, und löscht ihn selbständig wieder aus der Tabelle.

**Welche Protokolle können mit IP-Masquerading übertragen werden?**

Natürlich nur solche, die auch über Ports kommunizieren. Protokolle, die ohne Port-Nummern arbeiten oder die oberhalb von IP im OSI-Modell Ports verwenden, können nicht ohne spezielle Behandlung maskiert werden.

In der aktuellen Version führt der Router ein Masquerading für folgende Protokolle durch:

- TCP (und alle darauf aufbauenden Protokolle wie FTP, HTTP etc.)
- UDP
- ICMP

### 4.3.5 DNS-Forwarding

Beim Zugriff auf das Internet werden meistens keine IP-Adressen verwendet, um einen Server zu erreichen, sondern Namen. Wer weiß auch schon, welche Adresse sich hinter 'www.domain.com' verbirgt? Der DNS-Server!

DNS heißt Domain Name Service und bezeichnet die Zuordnung von Domain-Namen (wie domain.com) zu den entsprechenden IP-Adressen. Diese Informationen müssen natürlich ständig gepflegt und immer weltweit verfügbar gehalten werden. Dazu gibt es eben diese DNS-Server, die lange Tabellen mit IP-Adressen und Domain-Namen anbieten.

Wenn nun ein Rechner aus dem Intranet eine Homepage aufrufen möchte, sendet er zunächst einen DNS-Request aus: „Welche IP-Adresse gehört zu www.domain.com?"

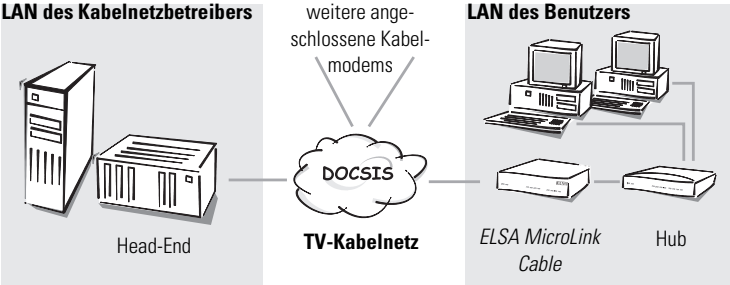
Wenn das Kabelmodem bei den Arbeitsplatzrechnern als DNS-Server eingetragen ist, wird diese Anfrage folgendermaßen behandelt:

- Das Gerät versucht einen DNS-Server beim Kabelnetzbetreiber zu erreichen, und holt die Zuordnung der IP-Adresse zum Namen von dort. Die Adresse des DNS beim Netzbetreiber wird bei der Anmeldung des Kabelmodems vom Head-End übermittelt.

Durch dieses Verfahren benötigen Sie keine Kenntnisse über die Adressen eines DNS-Servers. Der Eintrag der LAN-IP-Adresse des Kabelmodems als DNS-Server bei den Arbeitsplatzrechnern reicht aus, um die Namenszuordnung zu ermöglichen. Außerdem wird damit die Adresse des DNS-Servers automatisch aktualisiert. Sollte z.B. der Provider, der diese Adresse mitteilt, seinen DNS-Server umbenennen, oder Sie sollten zu einem anderen Provider wechseln, erhält Ihr lokales Netz stets die aktuellen Informationen.

### 4.3.6 Bridging

Eine Bridge verbindet zwei oder mehrere LANs so, daß sie nach außen hin wie ein großes Netzwerk erscheinen. Beim Bridging über Kabelmodems findet man auf der einen Seite das LAN des Kabelnetzbetreibers mit dem Head-End und auf der anderen Seite das LAN des Netzteilnehmers mit dem Kabelmodem und den lokalen Rechnern.




In der Betriebsart als Bridge überträgt ein *ELSA MicroLink Cable* alle Daten zu Rechnern, deren MAC-Adressen nicht lokal zugeordnet werden können, zwischen einem lokalen Netz (LAN) oder einem Arbeitsplatzrechner auf der einen Seite und dem Kabelnetz auf der anderen Seite.

Dabei lernt die Bridge selbständig, welche MAC-Adressen im LAN liegen. Beim Empfang der Daten aus dem Kabelnetz entscheidet die Bridge im Kabelmodem anhand der MAC-Adressen, ob die Daten für das eigene LAN bestimmt sind. Die Bridge läßt dann nur die Datenpakete durch, die an MAC-Adressen im eigenen LAN adressiert sind.

DE

*Die Filterung mit der genauen Angabe der MAC-Adressen verlangt natürlich auch einen gewissen Pflegeaufwand. Ändern sich die Adressen z.B. durch den Tausch einer Netzwerkkarte, dann müssen die neuen Adressen eingetragen werden, um die korrekte Funktion der Bridge aufrechtzuerhalten.*

## 4.4 Automatische Adreßverwaltung mit DHCP

Für einen reibungslosen Betrieb in einem TCP/IP-Netzwerk benötigen alle Geräte in einem lokalen Netzwerk eindeutige IP-Adressen.

Neben den IP-Adressen brauchen die Geräte im LAN noch die Adressen von DNS-Servern sowie eines Standard-Gateways, über das Datenpakete von lokal nicht erreichbaren Adressen geroutet werden sollen.

Bei einem kleinen Netzwerk ist es durchaus noch denkbar, allen Rechnern im Netz „von Hand" diese Adressen einzutragen. Bei einem großen Netz mit vielen Arbeitsplatzrechnern wird das jedoch leicht zu einer unüberschaubaren Aufgabe.

In solchen Fällen bietet sich die Verwendung des DHCP (Dynamic Host Configuration Protocol) an. Über dieses Protokoll kann ein DHCP-Server in einem TCP/IP-basierten LAN den einzelnen Stationen die benötigten Adressen dynamisch zuweisen.

Das Kabelmodem gehört im Prinzip zu zwei LANs:

- Auf der einen Seite ist es Teil des LANs beim Kabelnetzbetreiber und bildet mit dem Head-End und allen daran angeschlossenen Kabelmodems ein LAN. Die Zuweisung der IP-Adressen vom Kabelnetzbetreiber zum Teilnehmer erfolgt über DHCP.
- Auf der anderen Seite bildet das Kabelmodem mit einem oder mehreren angeschlossenen Rechnern ein eigenes LAN. Mit DHCP können auch innerhalb Ihres LANs die Adressen verwaltet werden.

Das Kabelmodem arbeitet also als DHCP-Client und als DHCP-Server.

### 4.4.1 Der DHCP-Client

Die Cable-IP-Adresse für den Datenaustausch im Kabelnetz wird während der Anmeldung beim Head-End über DHCP vom Kabelnetzbetreiber zugewiesen, der Netzteilnehmer hat i.d.R. keinen Einfluß darauf. Neben der LAN-IP-Adresse, die das Kabelmodem beim Betrieb im Kabelnetz verwenden soll, werden dabei noch einige weitere Informationen wie z.B. das Gateway ins Internet beim Kabelnetzbetreiber oder der Zeit-Server übermittelt.

Da diese Zuweisung über DHCP vom Kabelnetz zum Kabelmodem zwingend erforderlich ist, muß der DHCP-Client auch nicht konfiguriert werden. Im Menü `Status/DHCP-Client-Status` können die aktuellen Zuweisungen jederzeit abgelesen werden.

### 4.4.2 Der DHCP-Server

*ELSA MicroLink Cable* kann als DHCP-Server die IP-Adressen in seinem TCP/IP-Netz verwalten. Dabei teilt er den Arbeitsplatzrechnern die folgenden Parameter mit:

- IP-Adresse
- Netzmaske
- Broadcast-Adresse
- DNS-Server
- Default-Gateway
- Gültigkeitsdauer der zugewiesenen Parameter

Der DHCP-Server entnimmt die LAN-IP-Adressen entweder aus einem frei definierten Adreß-Pool oder ermittelt die Adressen selbständig aus der eigenen LAN-IP-Adresse.

### 4.4.3 DHCP – 'Ein', 'Aus' oder 'Auto'?

Der DHCP-Server in den Geräten von ELSA kann drei verschiedene Zustände annehmen:

- 'Ein': Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adreß-Pools) überprüft.
  - Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an.
  - Bei einer fehlerhaften Konfiguration (z.B. ungültige Pool-Grenzen) wird der DHCP-Server wieder abgeschaltet und wechselt in den Zustand 'Aus'.
- 'Aus': Der DHCP-Server ist dauerhaft abgeschaltet.
- 'Auto': Der Server befindet sich im Automodus. In diesem Zustand sucht das Gerät nach dem Einschalten im lokalen Netz nach anderen DHCP-Servern.
  - Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Damit wird u.a. verhindert,

daß ein unkonfiguriertes Gerät nach dem Einschalten im Netz Adressen vergibt, die nicht im lokalen Netz liegen.

- Im Bridge-Betrieb des Kabelmodems schaltet sich der DHCP-Server auch aus, sobald sich das Kabelmodem am Head-End angemeldet hat.
- Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein.

Ob der Server letztendlich ein- oder ausgeschaltet ist, kann den DHCP-Statistiken entnommen werden.

Die Default-Einstellung für den Zustand ist 'Auto'.

### 4.4.4 So werden die Adressen zugewiesen

**Zuweisung von IP-Adressen im LAN**

Damit der DHCP-Server den Rechnern im Netz IP-Adressen zuweisen kann, muß er zunächst einmal wissen, welche Adressen er für diese Zuweisung verwenden darf. Für die Auswahl der möglichen Adressen gibt es drei verschiedene Optionen:

- Die IP-Adresse kann aus dem eingestellten Adreß-Pool genommen werden (Start-Adreß-Pool bis End-Adreß-Pool). Hier können beliebige im lokalen Netz gültige Adressen eingegeben werden.
- Wird stattdessen '0.0.0.0' eingegeben, so ermittelt der DHCP-Server selbständig die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen für die LAN-IP-Adresse im 'TCP/IP-Modul'.
- Wenn das Kabelmodem keine eigene LAN-IP-Adresse hat, befindet sich das Gerät in einem besonderen Betriebszustand. Es verwendet dann selbst die IP-Adresse '10.0.0.254' und den Adreß-Pool '10.x.x.x' für die Zuweisung der IP-Adressen im Netz. In diesem Zustand weist der DHCP-Server den anderen Rechnern im Netz nur die IP-Adresse und deren Gültigkeit zu, nicht jedoch die anderen Informationen.

Wenn nun ein Rechner im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Gerät mit aktiviertem DHCP-Modul die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit bereits schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die ausgesuchte Adresse im lokalen Netz noch frei ist. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

**Zuweisung der Netzmaske**

Die Zuweisung der Netzmaske erfolgt analog zur Adreßzuweisung. Wenn im DHCP-Modul eine Netzmaske eingetragen ist, wird diese bei der Zuweisung verwendet. Ansonsten wird die Netzmaske aus dem TCP/IP-Modul verwendet.

**Zuweisung der Broadcast-Adresse**

In der Regel wird im lokalen Netz für Broadcast-Pakete eine Adresse verwendet, die sich aus den gültigen IP-Adressen und der Netzmaske ergibt. Nur in Sonderfällen (z.B. bei Verwendung von Sub-Netzen für einen Teil der Arbeitsplatzrechner) kann es nötig sein, eine andere Broadcast-Adresse zu verwenden. In diesem Fall wird die zu verwendende Broadcast-Adresse im DHCP-Modul eingetragen.

*Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen.*

**Zuweisung von DNS-Servern**

Die Adressen der DNS-Server werden während der Registrierung beim Head-End ausgehandelt und eingetragen.

**Zuweisung des Default-Gateways**

Der Router weist dem anfragenden Rechner immer seine eigene IP-Adresse als Gateway-Adresse zu.

Falls erforderlich, kann diese Zuweisung durch die Einstellungen am Arbeitsplatzrechner überschrieben werden.

**Gültigkeitsdauer einer Zuweisung**

Die dem Rechner einmal zugewiesenen Adressen haben nur eine begrenzte Gültigkeit. Nach Ablauf dieser Gültigkeitsdauer darf der Rechner sie nicht mehr verwenden. Damit der Rechner die Adressen (vor allem seine IP-Adresse) danach nicht immer wieder verliert, beantragt er rechtzeitig eine Verlängerung, die ihm in der Regel auch immer gewährt wird. Nur wenn die Gültigkeitsdauer abläuft, während der Rechner abgeschaltet ist, verliert er die Adresse.

Bei jeder Anfrage kann ein Host eine bestimmte Gültigkeitsdauer fordern. Ein DHCP-Server kann dem Host aber auch eine davon abweichende Gültigkeitsdauer zuweisen. Das DHCP-Modul bietet zwei Einstellungen, um die Gültigkeitsdauer zu beeinflussen:

- Maximale Gültigkeit in Minuten

  Hier kann die maximale Gültigkeitsdauer eingetragen werden, die der DHCP-Server einem Host zuweist.

  Fordert ein Host eine Gültigkeit an, die die maximale Dauer von 6.000 Minuten überschreitet, so wird ihm nur diese maximale Gültigkeit zugewiesen!

  Der Defaultwert von 6.000 Minuten entspricht ca. 4 Tagen.

- Default-Gültigkeit in Minuten

  Hier kann die Gültigkeitsdauer eingetragen werden, die zugewiesen wird, wenn der Host überhaupt keine Gültigkeitsdauer anfordert. Der Defaultwert von 500 Minuten entspricht ca. 8 Stunden.

### Vorfahrt für den DHCP-Server – Zuweisung anfordern

Standardmäßig sind fast alle Einstellungen in der Netzwerkumgebung von Windows so eingestellt, daß die benötigten Parameter über DHCP angefragt werden. Überprüfen Sie die Einstellungen mit einem Klick auf **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter, und öffnen Sie die **Eigenschaften**.

Auf den verschiedenen Registerkarten können Sie nun nachsehen, ob spezielle Einträge z.B. für die IP-Adresse oder das Standard-Gateway vorhanden sind. Wenn Sie alle Werte vom DHCP-Server zuweisen lassen wollen, löschen Sie nur die entsprechenden Einträge.

### Vorfahrt für den Rechner – Zuweisung überschreiben

Sollte ein Rechner andere Parameter verwenden als die ihm zugewiesenen (z.B. ein anderes Standard-Gateway), so muß es direkt am Arbeitsplatzrechner eingestellt werden. Der Rechner ignoriert dann die entsprechenden Parameter in der Zuweisung durch den DHCP-Server.

Unter Windows geschieht das z.B. über die Eigenschaften der Netzwerkumgebung.

Klicken Sie auf **Start ▶ Einstellungen ▶ Systemsteuerung ▶ Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter und öffnen die **Eigenschaften**.

Auf den verschiedenen Registerkarten können Sie nun die gewünschten Werte eintragen.

Im DCHP-Modul kann über den Punkt 'Setup/DHCP-Server-Modul/Tabelle-DCHP' die Zuweisung von IP-Adressen an die jeweiligen Rechner überprüft (bzw. nachgeschaut) werden. Diese Tabelle zeigt die zugewiesene IP-Adresse, die MAC-Adresse, die Gültigkeitsdauer, den Namen des Rechners (falls vorhanden) sowie den Typ der Adreßzuweisung.

Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:

- neu

  Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.

- unbek.

  Bei der Überprüfung der Eindeutigkeit wurde festgestellt, daß die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.

- stat.

  Ein Rechner hat dem DHCP-Server mitgeteilt, daß er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr verwendet werden.

- dyn.

  Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

DE

# 5 Technische Grundlagen

Dieses Kapitel gibt eine kurze Einführung in die Technik, die Ihr neues Gerät nutzt. Profis in Sachen Netzwerktechnik können sicher schnell über diese Abhandlungen hinweggehen, für Einsteiger bietet dieser Teil der Dokumentation jedoch eine nützliche Hilfe beim Verstehen der Fachbegriffe und Prozesse.

## 5.1 Die Technik der Kabelmodems

Kabelmodems gehören zu den neuen, breitbandigen und zukunftsorientierten Zugangstechnologien für das Internet. Anders als normale Modems oder ISDN-Modems nutzen diese Geräte für die Übertragung der Daten zwischen Internet-Nutzer und Provider nicht die Telefonleitungen, sondern die ebenfalls in fast allen Haushalten vorhandenen Breitbandkabel für die Fernseh- und Rundfunkübertragung.

***Downstream**: Übertragung der Daten vom Provider zum Internet-Nutzer*

Diese Kabel eignen sich ausgezeichnet für die Übertragung großer Datenmengen. Ein Problem war bisher die Beschränkung des Datenflusses in eine Richtung, nämlich vom Provider zum Nutzer (Downstream). Videotext funktioniert nach diesem Prinzip: Der Provider, in diesem Fall der Fernsehsender, stellt ein bestimmtes Informationsangebot in Form einzelner Seiten in sein Netz und sendet dieses permanent in das Kabelnetz.

***Upstream**: Übertragung der Daten vom Internet-Nutzer zum Provider*

Der Nutzer kann dann aus den angebotenen Seiten, z.B. durch Eingabe einer Nummer, eine gewünschte Seite auswählen. Der Benutzer ist allerdings auf das spezieller Angebot der Fernsehsender beschränkt und kann keine Daten zurücksenden (Upstream).

### 5.1.1 Standards

Zwei Standards umgehen dieses Problem:

- Die erste Lösung akzeptiert die Beschränkung auf den Downstream über das Kabelnetz und regelt den Upstream über normale Telefonleitungen. Der Nachteil liegt auf der Hand: Ein zusätzlicher Anschluß an das Telefonnetz (z.B. über ein normales Modem) ist erforderlich und taktabhängige Telefongebühren werden weiterhin berechnet.
- Der weltweit akzeptierte und eingesetzte Standard, rüstet das Kabelnetz mit geeigneten Verstärkern und Gegenstellen auch für den Datenrücktransport aus. Diese Gegenstellen heißen Head-End oder CMTS (**C**able

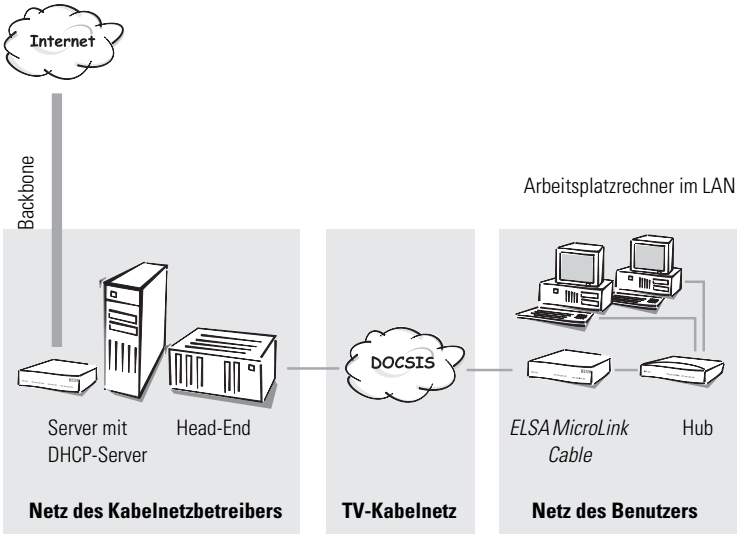
**M**odem **T**ermination **S**ystem). Die Verbindungen nach dem DOCSIS-Standard (**D**ata **O**ver **C**able **S**ystem **I**nterface **S**pecification) benötigen dann keine zusätzliche Telefonverbindung mehr. Der Zugriff auf das Internet ist damit zeitlich nicht mehr von einer bestimmten Taktrate abhängig, Sie haben quasi eine Standleitung ins Internet.

### 5.1.2 Der Zugang

Um den Zugang zum Internet über das Kabelnetz (anhand einer vereinfachten Darstellung) zu verdeutlichen, betrachten wir zunächst die beiden Seiten der Verbindung: Auf der einen Seite haben wir den Anwender, der mit einem einzelnen Rechner oder mit einem lokalen Netz das Internet nutzen möchte. Auf der anderen Seite haben wir den Betreiber eines TV-Breitband-Kabelnetzes, der seinen Kunden mehr als nur Radio und Fernsehen anbieten möchte.

An ein Head-End können sich in der Regel bis zu 2000 Teilnehmer mit einem Kabelmodem wie dem *ELSA MicroLink Cable* anschließen. Das Head-End arbeitet dabei allerding als Multiport, d.h., jeder Teilnehmer bekommt jederzeit einen Zugang zum Kabelnetz. Es kann also nicht wie beim Zugang über herkömmliche Modems oder ISDN-Modems vorkommen, daß der Internet-Nutzer vergeblich versucht, seinen Provider anzuwählen, weil schon alle Einwahlgegenstellen besetzt sind. Wenn sowohl das Kabelmodem als auch das Head-End den rückkanalfähigen DOCSIS-Standard beherrschen, wird für die Verbindung zwischen Internet-Nutzer und Kabelnetzbetreiber keine weitere Hardware benötigt.

Auf der anderen Seite muß der Netzbetreiber noch eine Verbindung ins Internet herstellen. Dazu kann er entweder selbst als Internet-Service-Provider (ISP) auftreten und direkt einen Anschluß an das Internet herstellen, oder er überträgt diese Aufgabe einem anderen Dienstleister, z.B. einem freien ISP oder einem Online-Dienst.




Für den Benutzer ist dieser Anschluß an den Backbone nur von geringer Bedeutung. Klar sein sollte aber folgendes: Je mehr Leistung der Kabelnetzbetreiber seinem Backbone-Leitung spendiert, desto schneller bekommen die Kunden die Informationen aus dem Internet.

## 5.1.3 Anmeldung im Kabelnetz

Das TV-Kabelnetz verfügt im Vergleich mit anderen Medien zur Datenübertragung über eine sehr hohe Bandbreite (daher auch der Begriff Breitband-Kabelnetz). Diese gesamte Bandbreite ist in verschiedene Kanäle eingeteilt, die für die Übermittlung von unterschiedlichen Informationen reserviert sind. Vom Fernsehen her kennen Sie das, da finden Sie die einzelnen Programme auf jeweils eigenen Kanälen. Auch für die Übertragung der Internet-Inhalte sind bestimmte Kanäle eingerichtet.

***Synchronisation**: Suche eines Kanals im Breitbandnetz*

Nach dem Einschalten sucht ein Kabelmodem zunächst den gesamten Frequenzbereich nach einem Kanal ab, auf dem der Netzbetreiber Informationen aus dem Internet sendet. Dieser Vorgang kann aufgrund der großen Bandbreite beim ersten Anmelden eine gewisse Zeit dauern. Ist der entsprechende Kanal aber gefunden, leuchtet am *ELSA MicroLink Cable* die Sync-LED auf. Beim nächsten Einschalten sucht das Kabelmodem zuerst wieder auf dem vorher gefundenen Kanal und findet so normalerweise wesentlich schneller die gesuchten Informationen. Wird das Kabelmodem jedoch beim

DE

nächsten Mal an einem anderen Anschluß betrieben, muß evtl. wieder der gesamten Frequenzbereich durchsucht werden.

Um die Suche etwas zu beschleunigen, kann der Kabelnetzbetreiber in einer Voreinstellung das *ELSA MicroLink Cable* auf die Suche in bestimmten Frequenzbereichen (Bändern) einstellen, die er normalerweise verwendet.

*Ändern Sie selbst diese Voreinstellung nicht ohne Rücksprache mit Ihrem Netzbetreiber.*

***Registrierung**: Austausch von Verwaltungsinformationen zwischen Head-End und Kabelmodem*

Wenn ein Kanal zur Kommunikation mit dem Netzbetreiber gefunden ist, teilt das Head-End dem Kabelmodem eine Reihe von Informationen mit, die für den Betrieb im Kabelnetz wichtig sind. Dieser Vorgang heißt auch Registrierung. Dazu gehören u.a.:

- die Bestätigung des gefundenen Kanals oder der Wechsel auf einen anderen Kanal
- die Zuweisung einer im Kabelnetz gültigen IP-Adresse mit passender Netzmaske
- die Information über die Adressen der Server beim Netzbetreiber
- die aktuelle Zeit

Wenn die Registrierung erfolgreich abgeschlossen ist, leuchtet am *ELSA MicroLink Cable* die Reg'd-LED auf, und das Kabelmodem ist bereit für den Zugang zum Internet.

## 5.2 Netzwerktechnik

*Dieser Abschnitt stellt in kurzen Worten einige Grundlagen der Netzwerktechnik vor. Diese Erläuterungen erklären **nicht alle** möglichen Techniken, Verfahren und Begriffe, die im Zusammenhang mit der Netzwerktechnik verwendet werden, sondern nur, soweit sie für das Verständnis der anderen Produktinformationen notwendig oder hilfreich sind.*

### 5.2.1 Das Netzwerk und seine Komponenten

*Netzwerk, Übertragungsmedium, Schnittstellen*

Wenn mehrere Rechner untereinander kommunizieren, wird dieser Verbund als „Netzwerk" bezeichnet. Damit Rechner untereinander kommunizieren können, benötigen sie ein physikalisches Medium, über das die Informationen übertragen werden. Das können z.B. Kabel- oder Funkverbindungen sein, die über spezielle Schnittstellen (z.B. Netzwerkkarten) mit den Rechnern verbunden werden.

DE

*Wenn im folgenden der Begriff Netzwerkkabel (oder nur Kabel) verwendet wird, ist damit auch jedes andere physikalische Medium gemeint, das die Funktion der Kabel übernehmen kann, wie z.B. Funkstrecken.*

*Pakete, Zellen*

Die einzelnen elektronischen Informationen, die über ein Medium von einem Rechner zum anderen geschickt werden, bezeichnet man je nach Verfahren als Pakete oder als Zellen.

*Für die meisten der folgenden Erläuterungen ist der Unterschied zwischen Paketen und Zellen nicht relevant. Wir verwenden also allgemein den Begriff Pakete oder Datenpakete, und gehen nur an den entsprechenden Stellen näher auf die speziellen Eigenschaften von Zellen ein.*

*Host*

Die Rechner und andere Endgeräte (z.B. Drucker) in einem Netzwerk, die Informationen erzeugen oder verarbeiten, heißen Host. Idealerweise ist ein Host von der Aufgabe befreit, Informationen weiterzuleiten. Ein Host hat in der Regel genau eine Schnittstelle, mit der er am Netzwerk angeschlossen ist.

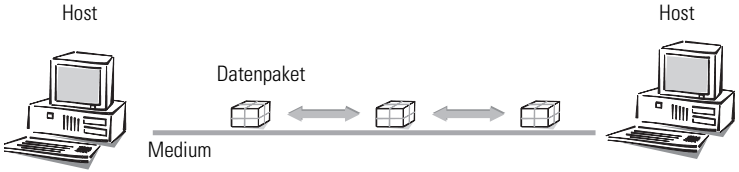
*Router*

Der Transport von Paketen zwischen zwei Hosts erfolgt indirekt über Vermittlungsstellen, die ein Paket zum Zielrechner weiterreichen. Diese Vermittlungsstellen heißen Router. Ein Router hat mindestens zwei Schnittstellen, damit er die Daten von einem Sender in Empfang nehmen kann und an einen Empfänger weiterleiten kann. Ein Router hat neben der Vermittlungsfunktion auch immer die Eigenschaften eines Hosts, damit er selbst das Ziel von Datenpaketen sein kann, z.B. zum Zweck der Konfiguration.

## 5.2.2 Verbindungsarten

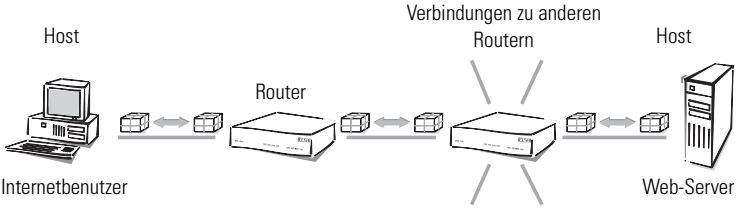
*Punkt-zu-Punkt-Verbindung*

Werden genau zwei Hosts über ein Medium verbunden, spricht man von „Punkt-zu-Punkt-Verbindungen". Dabei schickt ein Host Pakete ab, die nur bei genau **einem** Empfänger ankommen können (eindeutige Verbindung).




Auch bei einem Zugriff auf das Internet handelt es sich um eine Punkt-zu-Punkt-Verbindung. Die Datenpakete werden zwar vom Host beim Internetbenutzer über mehrere Router zum Host (Server) beim Internet-Provider gesen-

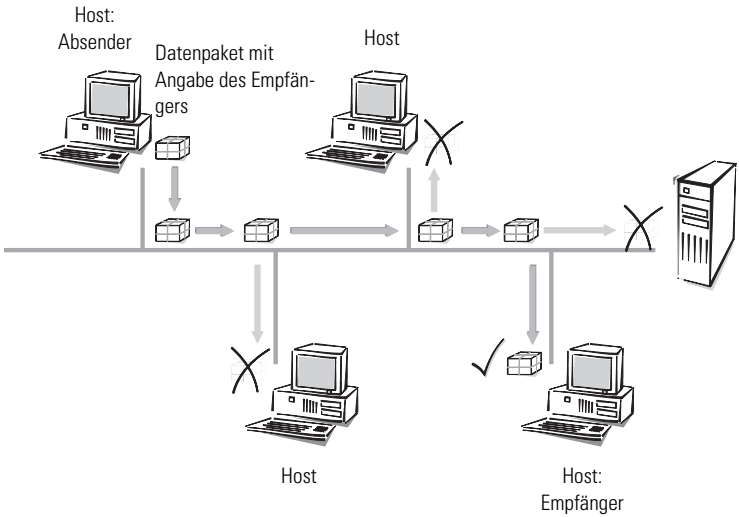
det, jedes Datenpaket hat jedoch ein ganz bestimmtes Ziel. Die Router geben die Datenpakete auch nur an genau einen Empfänger weiter. Daher bezeichnen wir auch diese Verbindung als eindeutig.




*Der Begriff der „Punkt-zu-Punkt-Verbindung" ist strenggenommen nicht ganz korrekt. Für unsere Betrachtungen reicht es jedoch aus, diese Art der Verbindung gegen die folgenden „Punkt-zu-Mehrpunkt-Verbindungen" abzugrenzen.*

*Punkt-zu-Mehrpunkt-Verbindung*

In der Regel ist es unwirtschaftlich, alle Rechner eines Netzes durch Punkt-zu-Punkt-Kabel direkt miteinander zu verbinden, da dann jeder Rechner eine Vielzahl von Schnittstellen besitzen müßte. Daher schließt man die Rechner in dem Netzwerk an ein gemeinsames Medium an, das sich alle Hosts teilen. Der Absender schickt sein Paket mit der Angabe des Empfängers einfach los auf das Medium, an das mehrere Hosts angeschlossen sind. Das Datenpaket kommt bei **jedem** Host im Netzwerk an, der dann entscheidet, ob er selbst der Empfänger des Paketes ist oder nicht. Ist das Paket an den entsprechenden Host gerichtet, nimmt er es an, ansonsten beachtet er es nicht (er verwirft es). Dabei handelt es sich um eine nicht eindeutige Verbindung, man spricht von „Punkt-zu-Mehrpunkt-Verbindungen".




## 5.2.3 Netzwerk-Arten

*Protokoll*

Eine wichtige Voraussetzung für die Rechnerkommunikation ist eine gemeinsame Sprache der Hosts untereinander. Diese Sprachen nennt man in der Netzwerktechnik „Netzwerkprotokoll" oder kurz „Protokoll".

*TCP/IP*

Das am weitesten verbreitete Netzwerkprotokoll ist das TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol). Es wird vorrangig im Internet benutzt, ist heute aber auch oft in Firmennetzwerken zu finden. Andere Netzwerkprotokolle sind z.B. IPX oder AppleTalk. Wegen der großen Verbreitung wird in diesem Kapitel hauptsächlich das TCP/IP betrachtet.

*IP-Netz*

Alle Hosts, die über das TCP/IP-Protokoll kommunizieren wollen, müssen zu einem gemeinsamen Netzwerk zusammengeschlossen sein und das TCP/IP-Protokoll (auch TCP/IP-Stack genannt) installiert haben. Ein solches Netz wird als IP-Netz bezeichnet.

*Internetwork*
*Internet*

Der Verbund mehrerer Netzwerke, die auf dem IP-Protokoll basieren, wird als Internetwork bezeichnet. Der größte Zusammenschluß von vielen kleinen, öffentlichen IP-Netzwerken ist das Internet.

*Lokales Netzwerk (LAN)*

Ein Netzwerk von begrenzter räumlicher Ausdehnung, bei dem die Hosts gleichberechtigt ein gemeinsames Medium nutzen (Shared Medium), ist ein lokales Netzwerk (engl. **L**ocal **A**rea **N**etwork, LAN).

DE

## 5.3 IP-Adressierung

*Paketorientierte Übertragung*

In IP-Netzen erfolgt die Kommunikation zwischen Rechnern paketorientiert. Dabei werden Daten oder Nachrichten in Pakete variabler Länge verpackt und als Ganzes von einem Quellrechner zu einem Zielrechner transportiert. Ein Datenpaket enthält neben den eigentlich zu übertragenden Informationen (Nutzdaten) auch Kontroll- und Adressierungsinformationen.

*IP-Adresse*

In IP-Netzen werden IP-Adressen zur Kommunikation zwischen verschiedenen Geräten verwendet. Jeder Host hat dabei seine eigene Adresse, mit der er eindeutig identifiziert werden kann. Wie sieht nun eine IP-Adresse aus? Sie besteht aus vier Bytes, die durch Punkte getrennt sind, insgesamt also aus 32 Bits. Jedes der vier Bytes kann Werte von 0 bis 255 annehmen, z.B. 192.168.130.124.

*Exakt betrachtet bezeichnet eine IP-Adresse nicht den Host, sondern seine Schnittstelle. Hat ein Endgerät im Netzwerk mehrere Schnittstellen (wie z.B. Router), so muß es für jede Schnittstelle eine eigene IP-Adresse besitzen. Deshalb haben ELSA MicroLink Cable im Router-Betrieb sowohl eine IP-Adresse zur Kommunikation mit den Hosts im LAN als auch eine zweite IP-Adresse zur Kommunikation mit der „Außenwelt" über TV-Kabelnetz.*

*Netzwerkadresse*

In einer IP-Adresse ist sowohl die Adresse des Netzwerks enthalten als auch die des Hosts. Die Netzwerkadresse ist für alle Hosts in einem Netzwerk gleich, die Adresse eines Hosts ist einmalig und eindeutig in einem Netzwerk. Ein Router z.B. kann mehrere verschiedene, im Netzwerk eindeutige IP-Adressen haben.

*Netzmaske*

Wie unterscheidet man nun den Teil, der das Netzwerk bestimmt, und den Teil, der den Host identifiziert? Mit Hilfe der Netzmaske. Masken kennen Sie alle: Die decken einen Teil von etwas ab und lassen nur den anderen Teil sichtbar werden. Genau so verhält es sich mit der Netzmaske. Das ist eine Zahl mit dem gleichen Aufbau wie die IP-Adresse, also 32 Nullen oder Einsen. Die Netzmaske fängt meistens vorne mit Einsen an und hört hinten mit Nullen auf. Die Nullen am Ende decken dabei den Teil der IP-Adresse ab, der nicht zur Netzwerkadresse gehört.

Beispiele:

| Diese Adresse ... | ... in Bytes ... | ... sieht in Bits so aus: |
|---|---|---|
| IP-Adresse | 192.168.120.253 | 11000000.10101000.01111000.11111101 |
| Netzmaske | 255.255.255.0 | 11111111.11111111.11111111.00000000 |

| Diese Adresse ... | ... in Bytes ... | ... sieht in Bits so aus: |
|---|---|---|
| Netzwerk-Adresse | 192.168.120.0 | 11000000.10101000.01111000.00000000 |

Die gleiche IP-Adresse, jetzt mit anderer Netzmaske:

| Diese Adresse ... | ... in Bytes ... | ... sieht in Bits so aus: |
|---|---|---|
| IP-Adresse | 192.168.120.253 | 11000000.10101000.01111000.11111101 |
| Netzmaske | 255.255.0.0 | 11111111.11111111.00000000.00000000 |
| Netzwerk-Adresse | 192.168.0.0 | 11000000.10101000.00000000.00000000 |

Sie sehen also: Eine IP-Adresse alleine ist noch nicht ausreichend. Nur im Zusammenspiel mit der Netzmaske kann ein Host eindeutig bezeichnet werden.

Und Sie sehen weiter: Je weniger Bits in der Netzmaske eine Eins enthalten, um so mehr Bits bleiben übrig zur Identifizierung der einzelnen Hosts in einem zusammenhängenden Netzwerk. Während im ersten Beispiel mit der Netzmaske 255.255.255.0 nur 254 verschiedene Adressen vergeben werden können sind es im zweiten Beispiel schon 254x254= 64516 verschiedene Adressen! Die erste und die letzte Ziffer eines Adreßraums sind jeweils reserviert für die Netzwerkadresse und die Broadcastadresse (Adresse für Pakete an alle Hosts in einem IP-Netz). Bei der Netzmaske 255.255.255.0 sind das die '0' für die Netzwerkadresse und die '255' als Broadcastadresse.

Eine neuere Schreibweise der Netzmaske hängt einfach die Anzahl der Bits, die für die Netzwerkadresse stehen, an die IP-Adresse an: 137.226.4.101/24. Die Zahl hinter dem Schrägstrich zeigt an, daß die ersten 24 Bits die Netzwerkadresse angeben. Mit dieser Schreibweise wird die Länge der Einträge in den Routingtabellen reduziert.

*Verwaltung der IP-Adressen*

Um Irrtümer zu vermeiden, müssen die IP-Adressen innerhalb eines zusammenhängenden Netzes eindeutig sein. Da auch das Internet mit vielen Millionen angeschlossener Rechner auf TCP/IP aufsetzt und damit IP-Adressen verwendet, müssen auch alle Adressen im Internet eindeutig sein. Zur Kontrolle dieser öffentlich zugänglichen Adressen gibt es Stellen, die die IP-Adressen verwalten und verteilen. Da die Anzahl der theoretisch verfügbaren IP-Adressen begrenzt ist, lassen sich die vergabeberechtigten Stellen die IP-Adressen teuer bezahlen.

*Private Address Spaces*

Damit eine Firma mit einem eigenen IP-Netzwerk aber nicht für jeden Arbeitsplatz eine IP-Adresse kaufen muß, sind bestimmte Bereiche der IP-Adressen

für die kostenlose Verwendung reserviert (Private Address Spaces). Diese Adressen können in einem abgeschlossenen Netz beliebig benutzt werden, z.B. in einem privaten Netz oder im Netz einer Firma. Innerhalb dieses Netzes müssen die IP-Adressen zwar eindeutig sein, aber in einem anderen abgeschlossenen Netzwerk (z.B. in einer anderen Firma) können die gleichen IP-Adressen zum Einsatz kommen.

Diese reservierten IP-Adressen dürfen jedoch **nicht** nach außen (ins Internet) bekannt gemacht werden. Nur **die** Geräte in einem Netzwerk, die Verbindung mit öffentlichen Netzwerken haben (z.B. Router an der Schnittstelle zum Internet), müssen eine registrierte IP-Adresse haben.

Bei der Vergabe von IP-Adressen, kontrolliert durch die IANA (**I**nternet-**A**ssigned-**N**umbers-**A**uthority), wurden die folgenden vier Adreßbereiche für nicht öffentliche IP-Netzwerke reserviert:

| IP-Adressen | Netzmaske | Bemerkung |
|---|---|---|
| 10.0.0.0 | 255.0.0.0 | „10er" Netze: Alle IP-Adressen, die mit einer 10. beginnen und deren Netzmaske mit 255. beginnt, fallen in den für private Netzwerke reservierten Adreßbereich. |
| 172.16.0.0 | 255.240.0.0 | Alle IP-Adressen, die mit 172.16.–172.31. beginnen und deren Netzmaske größer oder gleich 255.240.0.0 ist, fallen in den für private Netzwerke reservierten Adreßbereich. |
| 192.168.0.0 | 255.255.0.0 | Alle IP-Adressen, die mit 192.168. beginnen und deren Netzmaske mit 255.255. beginnt, fallen in den für private Netzwerke reservierten Adreßbereich. |
| 224.0.0.0 | 224.0.0.0 | Alle IP-Adressen, die mit 224. beginnen und deren Netzmaske ebenfalls mit 224. beginnt, fallen in den reservierten Adreßbereich.<br>Dieser Bereich ist reserviert für Broadcasts und sollte nicht für private Netze verwendet werden. |

Bei der Verwendung von IP-Adressen aus einem Private Address Space sind zwei Dinge zu beachten:

- Die im privaten Netzwerk verwendeten IP-Adressen (aus dem Private Address Space) dürfen dieses IP-Netzwerk nicht verlassen; d.h., ein Anschluß an das Internet ist nur mit zusätzlichen Hilfsmitteln (z.B. IP-Masquerading) möglich.
- Im Internet werden Pakete für diese IP-Adressen nicht geroutet, d.h., jeder Backbone-Router im Internet verwirft solche IP-Pakete stillschwei-

gend. Evtl. kann die Einschleusung solcher IP-Pakete ins Internet sogar schwerwiegende Konsequenzen nach sich ziehen (abhängig vom Vorgehen des jeweiligen Providers).

### 5.3.1 IP-Routing und hierarchische IP-Adressierung

*Routing*

Jedes IP-Paket enthält die IP-Adressen von Quelle und Ziel. Ein Router nimmt an seinen Schnittstellen IP-Pakete entgegen, interpretiert die Zieladresse und leitet die Pakete an diejenige seiner Schnittstellen weiter, die dem Ziel „am nächsten" ist. Das Finden des geeigneten Weges wird als Routing bezeichnet.

*Routingtabelle*

Für das Routen verwaltet jeder Router eine Tabelle (Routingtabelle). Sie bezeichnet für jeden Host im Netz die Router-Schnittstelle, über die der Host am schnellsten zu erreichen ist. Es ist leicht vorstellbar, daß mit wachsender Netzgröße diese Tabellen die Kapazität der Router sprengen (das Internet als weltweiter Verbund von öffentlich erreichbaren IP-Rechnern enthält mehrere Millionen Hosts).

*hierarchische IP-Adressen*

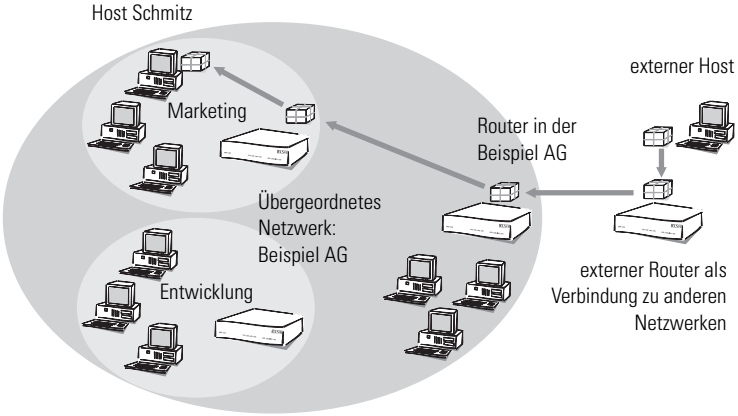
Aus diesem Grunde wurden hierarchische IP-Adressen eingeführt. Dazu wird das IP-Netz in Teilnetze unterteilt, in denen IP-Adressen aus einem zusammenhängenden Nummernraum vergeben werden. Es sind mehrere Hierarchie-Ebenen möglich, so daß mehrere Teilnetze zu größeren Teilnetzen zusammengefaßt werden können. Dies ist vergleichbar mit der hierarchischen Adresse bei der Briefpost, die aus Land, Stadt, Straße und Hausnummer besteht.

Die Konsequenzen dieser hierarchischen IP-Adressierung:

- Da die Netzwerkadresse innerhalb eines Netzwerks für alle Hosts gleich ist, reicht für die Kommunikation der Hosts untereinander in einem Netzwerk die Hostadresse aus.
- Ein Router muß zum einen die Adressen der Hosts kennen, die direkt an ihn angeschlossen sind, zum anderen muß der Router die Adressen aller Netze und Teilnetze kennen, die über benachbarte Router zu erreichen sind.

DE

- Ein Router muß **nicht alle** möglichen weiteren IP-Adressen kennen.




So kann z.B. eine Firma ein großes Netzwerk haben, in das die einzelnen Abteilungen als kleinere Teilnetze eingebunden sind. Die Adresse des Netzwerks für die Abteilung Marketing würde sich hierarchisch zusammensetzen aus der Adresse der Firma und der Abteilung.

Wenn ein Host außerhalb des Firmennetzes nun ein Paket an einen Host in der Beispiel AG senden möchte, passiert folgendes:

① Der Absender gibt dem Paket die Zieladresse „Host Schmitz – Marketing – Beispiel AG".

② Ein externer Router, der die Verbindung zu anderen Netzen herstellt, muß nur wissen, wie er die Beispiel AG erreicht. Sobald er ein Paket mit der Adresse für die Beispiel AG empfängt, leitet er das Paket an den Router weiter, der für die Beispiel AG zuständig ist.

③ Der Router in der Beispiel AG empfängt das Paket und entnimmt der Adresse die Information, daß es für die Beispiel AG gedacht ist. Weil er selber Teil der Beispiel AG ist, betrachtet er die Adresse genauer und sucht nach dem Namen der Abteilung. Dann leitet er das Paket weiter an den Router im Marketing.

④ Der Router im Marketing empfängt das Paket und entnimmt der Adresse die Information, daß es für das Marketing in der Beispiel AG gedacht ist. Weil er selber Teil dieser Abteilung ist, betrachtet er die Adresse genauer und sucht nach dem Namen des Hosts. Dann leitet er das Paket weiter an den Host von Mitarbeiter Schmitz.

Nun wollen wir das Beispiel einmal mit richtigen IP-Adressen betrachten und nicht mit den symbolischen Namen. Das Netzwerk der Beispiel AG verfügt über den Nummernraum '192.168.100.0' bis '192.168.100.255', mit der '0' als Netzwerkadresse und der '255' als Broadcastadresse.

Ein Router muß sich nur merken, daß alle Adressen, die mit '192.168.100' beginnen, im Netzwerk der Beispiel AG liegen.

Stellen wir uns jetzt einen Router vor, der mit einer Schnittstelle an das Netz der Beispiel AG angeschlossen ist. Empfängt er ein Paket mit Zieladresse '192.168.100.4' und Netzmaske '255.255.255.0', vergleicht er diese mit jeder ihm bekannten Netzwerkadresse. Dabei führt er ein logisches UND mit der Netzmaske aus und vergleicht das Ergebnis mit der Netzwerkadresse: '192.168.100.4' UND '255.255.255.0' ergibt '192.168.100.0'. Dies ist die Netzwerkadresse vom Netzwerk der Beispiel AG. Der Router erkennt, daß sich das Ziel in der Beispiel AG befindet und reicht das Paket an die Schnittstelle weiter, über die die Beispiel AG erreichbar ist. Innerhalb der Beispiel AG wird das Paket dann in das entsprechende Teilnetz weitergeleitet.

Bei der Übertragung von IP-Paketen innerhalb eines Netzwerks funktioniert das Verfahren auch:

① Wenn ein Host im Teilnetz der Entwicklung ein Datenpaket an Herrn Schmitz senden möchte, gibt der Absender dem Paket die Zieladresse „Host Schmitz – Marketing – Beispiel AG".

② Der Router in der Entwicklung empfängt das Paket und entnimmt der Adresse die Information, daß es für das Marketing in der Beispiel AG gedacht ist. Weil er selber Teil der Beispiel AG, nicht jedoch der Abteilung Marketing ist, leitet er das Paket weiter an den Router im übergeordneten Netzwerk.

③ Der Router in der Beispiel AG empfängt das Paket und entnimmt der Adresse die Information, daß es für die Beispiel AG gedacht ist. Weil er selber Teil der Beispiel AG ist, betrachtet er die Adresse genauer und sucht nach dem Namen der Abteilung. Dann leitet er das Paket weiter an den Router im Marketing, wo das Paket an den Empfänger weitergeleitet wird.

## 5.3.2 Erweiterung durch lokale Netze

*Medium Access Control*

Bisher haben wir nur Punkt-zu-Punkt-Verbindungen betrachtet. Viele Rechnernetze basieren jedoch auf Mehrpunkt-Verkabelungen wie dem Ethernet. Dabei können alle an ein gemeinsames Medium angeschlossenen Rechner

die Signale aller anderen Rechner empfangen (sogenannte Broadcast-Übertragung auf einem Shared Medium). Wenn mehrere Rechner gleichzeitig senden, überlagern und zerstören sich die einzelnen Signale. Zum Vermeiden und Auflösen derartiger Kollisionen wird ein Zugriffsprotokoll (engl. **M**edium **A**ccess **C**ontrol, MAC) eingesetzt.

*LAN und IP-Netz*

Der Verbund aller Rechner, die mittels eines MAC-Protokolls über ein Shared Medium kommunizieren, wird als LAN bezeichnet. Ein LAN bildet ein eigenständiges Netz und ist dem IP-Netz logisch untergeordnet, d.h., IP-Netze können die physikalischen Verbindungen eines LANs verwenden, um Verbindungen zwischen Hosts und Routern herzustellen. Ein LAN ist in der Regel räumlich und von der Anzahl der Netzteilnehmer auf wenige 10 bis 100 Hosts begrenzt, während ein IP-Netz theoretisch beliebig viele Hosts und Router verbinden kann (z.B. Internet).

*MAC-Adresse*

Zur Organisation der Übertragung im LAN werden spezifische LAN-Adressen verwendet, die vom Hersteller der Schnittstellenhardware fest einprogrammiert werden. Da die LAN-Adressen für die Kommunikation über das MAC-Protokoll verwendet werden, heißen Sie auch MAC-Adressen. Man kann sie sich wie einen Fingerabdruck der Schnittstellenhardware vorstellen. MAC-Adressen sehen z.B. so aus: 00-80-C7-6D-A4-6E.

MAC-Adressen sind unabhängig von IP-Adressen. Ein IP-Host, dessen Schnittstelle über ein LAN arbeitet, hat eine IP- und eine MAC-Adresse. Während IP-Adressen durch ihre Postadressen-ähnliche Struktur dafür ausgelegt wurden, das Routen in riesigen IP-Netzen zu vereinfachen, wurden Fingerabdruck-ähnliche MAC-Adressen darauf ausgelegt, den Anschluß eines neuen Rechners an ein LAN so einfach wie möglich zu gestalten.

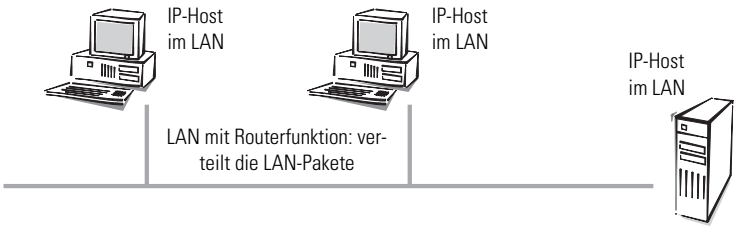
Auch in LANs wird paketorientiert übertragen. Jedes Paket enthält die MAC-Adresse von Quelle und Ziel. Zwar wird jedes Paket von allen Rechnern empfangen, jedoch nur von dem Zielrechner weiterverarbeitet. Zusätzlich gibt es eine spezielle MAC-Broadcast-Adresse, die von allen Rechnern im LAN weiterverarbeitet wird.

*IP im LAN*

Jedes LAN-Paket enthält einen Eintrag mit dem Typ des Netzwerkprotokolls. Ein IP-Paket kann z.B. über ein LAN übertragen werden, indem es in ein LAN-Paket verpackt und mit dem Protokoll-Typ 'IP' versehen wird. Die LAN-Schnittstelle im empfangenden Host erkennt anhand des IP-Eintrags, daß in dem LAN-Paket ein IP-Paket steckt, extrahiert es und verarbeitet es wie ein normales IP-Paket weiter. Auf diese Weise können über dasselbe LAN gleichzeitig IP-Pakete und Pakete anderer Netzprotokolle wie IPX übertragen wer-

den, ohne daß es zu Konflikten kommt (man sagt daher, daß ein LAN multiprotokollfähig ist).

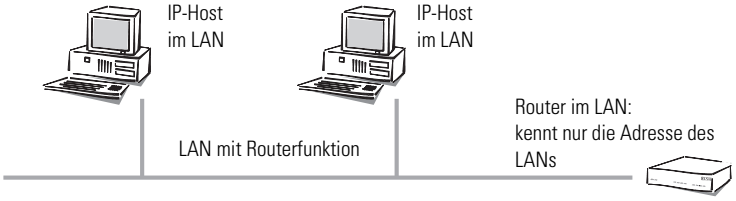
Für einen IP-Host verhält sich ein LAN so, also ob es ein eigenes Netzwerk mit einem Router wäre. Die Hosts geben die Pakete an das LAN ab, das die weitere Verteilung der Datenpakete übernimmt. Für die Kommunikation der Hosts untereinander über das IP-Protokoll dürfen in eim LAN somit nur IP-Adressen aus dem Nummernraum dieses Netzes verwendet werden.




Für einen Router im LAN erscheint ein Host im eigenen LAN, als wenn er hinter sich einem weiteren Router befindet. Der Router steht also vor einer einfachen Aufgabe: Da er für den Betrieb im IP-Netz nur die IP-Adressen

- der direkt angeschlossenen Hosts und
- die der erreichbaren Netze und Teilnetze

kennen muß, muß er sich also nur die Netzwerkadresse und die Netzmaske des Teilnetzes im LAN merken.




Der Host steht dagegen vor einer schwierigeren Aufgabe als der Router. Bei einer Schnittstelle mit Punkt-zu-Punkt-Kabel weiß ein Host, daß alle Pakete, die er über die Schnittstelle verschickt, automatisch z.B. bei seinem Router ankommen. Bei der Punkt-zu-Mehrpunkt-Verbindungen zum LAN muß er nun aber zwei Fälle unterscheiden.

- Ein Paket mit einer Zieladresse außerhalb des eigenen LANs gibt der sendende Host an einen Router im LAN weiter, der sich um die weitere Verarbeitung des Pakets kümmert.
- Ein Paket mit einer Zieladresse im eigenen LAN muß der sendende Host direkt an den Ziel-Host senden, denn ein Router im Netz kennt nicht die Adressen der einzelnen Hosts.

### Datenübertragung im eigenen LAN

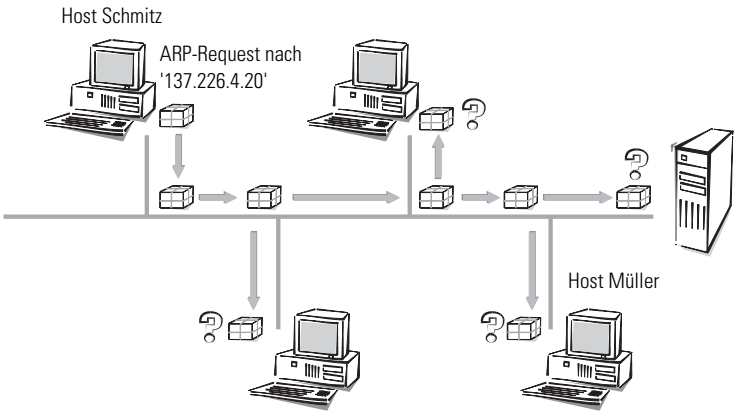
Veranschaulichen wir uns das an einem Beispiel. Stellen wir uns vor, daß die Hosts des Teilnetzes im Marketing über ein LAN verkabelt sind. Die Hosts haben IP-Adressen aus dem Nummernraum '137.226.4.1' bis '137.226.4.254' (die Adressen '137.226.4.0' und '137.226.4.255' sind reserviert), die Netzwerkadresse ist '137.226.4.0' und die Netzmaske '255.255.255.0'. An das LAN ist ein Router angeschlossen, der den Übergang in die weite Welt des Internet bildet. Seine LAN-Schnittstelle hat die IP-Adresse '137.226.4.1' und die MAC-Adresse '00-80-C7-6D-A4-6E'.

Stellen wir uns jetzt der Aufgabe, ein IP-Paket von Host Schmitz (mit IP-Adresse '137.226.4.10' und MAC-Adresse '00-10-5A-31-20-DF') an Host Müller (mit IP-Adresse '137.226.4.20' und MAC-Adresse '00-10-5A-31-20-EB') zu übertragen. Host Schmitz erkennt anhand der Netzwerkadresse und Netzmaske, daß Host Müller im Teilnetz des eigenen LANs ist. Er muß das Paket somit direkt über das LAN an Host Müller schicken. Leider kann er der LAN-Schnittstelle nicht sagen: „Schicke das IP-Paket an IP-Adresse 137.226.4.20", denn die LAN-Schnittstelle versteht nur MAC-Adressen.

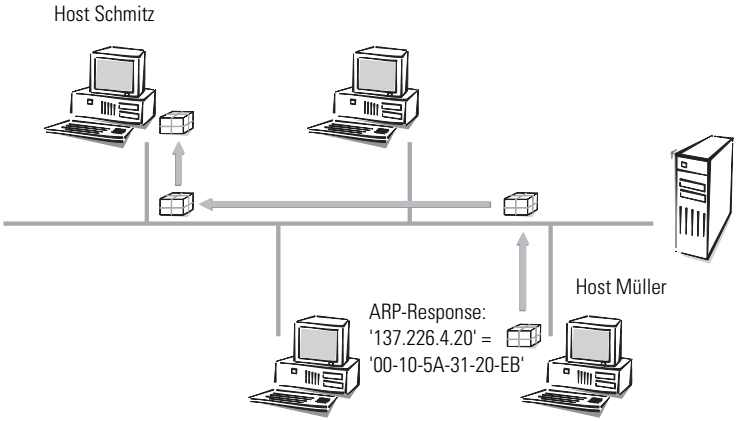
Jeder Host muß daher eine Tabelle verwalten, die IP-Adressen in MAC-Adressen übersetzt. Aber wie kommen die Einträge in die Tabelle? Sie könnten zwar von Hand eingetragen werden, aber das widerspricht der Vorgabe, den Anschluß eines neuen Rechners an ein LAN so einfach wie möglich zu gestalten.

*ARP*

Daher gibt es im LAN einen speziellen Mechanismus, der dies automatisiert: das **A**dress-**R**esolution-**P**rotokoll, ARP. Die Tabelle selbst wird ARP-Tabelle genannt. Immer wenn ein Host für eine IP-Adresse (in unserem Beispiel '137.226.4.20') keinen Eintrag in der ARP-Tabelle findet, verschickt er ein ARP-Request-Paket an alle Hosts im LAN (mit der LAN-Broadcastadresse als Zieladresse).




Dieses ARP-Request-Paket ist nichts anderes als die Frage an alle, wer denn auf die IP-Adresse '137.226.4.20' hört. Host Müller empfängt das Paket, fühlt sich angesprochen und antwortet mit einem ARP-Response-Paket, das er direkt an Host Schmitz verschickt (die MAC-Adresse '00-10-5A-31-20-DF' von Host Schmitz entnimmt er dem Absenderfeld im ARP-Request-Paket). Host Schmitz erkennt dies als Antwort auf seine Anfrage, entnimmt dem Absenderfeld des ARP-Response-Paketes die MAC-Adresse '00-10-5A-31-20-EB' von Host Müller und trägt sie in seine ARP-Tabelle ein.




Anschließend kann er sich endlich seiner ursprünglichen Aufgabe zuwenden, das IP-Paket an Host Müller zu verschicken. Er findet jetzt in der ARP-Tabelle den Eintrag „IP-Adresse 137.226.4.20 entspricht MAC-Adresse '00-10-5A-31-

20-EB'" und sagt seiner LAN-Schnittstelle: „Verschicke dieses IP-Paket an den Rechner mit der MAC-Adresse '00-10-5A-31-20-EB'".

### Datenübertragung aus dem eigenen LAN ins Internet

Stellen wir uns jetzt der zweiten Aufgabe, ein IP-Paket von Host Schmitz an einen weit entfernten Host Extern mit IP-Adresse 151.189.12.43 zu übertragen. Host Schmitz vergleicht die IP-Adresse mit seiner Netzwerkadresse und erkennt, daß Host Extern sich nicht im eigenen LAN befindet. Somit ist Host Extern nur über den Router zu erreichen. Die MAC-Adresse des Routers '00-80-C7-6D-A4-6E' erfährt er über dessen IP-Adresse durch Nachschauen in der ARP-Tabelle (ggf. vorher noch ein ARP-Request). Somit sagt Host Schmitz zu seiner LAN-Schnittstelle: „Verschicke dieses IP-Paket an den Rechner mit der LAN-Adresse '00-80-C7-6D-A4-6E'". Der Router entnimmt dem LAN-Paket das IP-Paket und liest daraus die IP-Adresse von Host Extern. In der Routingtabelle sucht der Router dann nach der Netzwerkadresse von diesem Host und findet so die Schnittstelle, über die er das IP-Paket weiterleiten muß.

### LAN-Kopplung auf MAC-Basis

Sie wissen, daß LANs das Anschließen von Rechnern an ein lokales Netz stark vereinfachen. Daher basieren fast alle Hausnetze auf LANs. Es gibt Situationen, wo einzelne LANs räumlich so weit ausgedehnt sind, daß die physikalischen Eigenschaften des Kabels den Anschluß weiterer Rechner behindern. Daraus ergibt sich der Bedarf, mehrere LANs so miteinander zu koppeln, daß sie elektrisch und bezüglich des MAC-Protokolls wie getrennte LANs agieren, aber gegenüber dem IP-Protokoll wie ein einziges großes LAN erscheinen.

Diese Koppelung von LANs erfolgt durch Bridges. Eine Bridge arbeitet ähnlich wie ein Router, verwendet zur Wegefindung jedoch keine IP-Adressen, sondern ausschließlich MAC-Adressen. Da die MAC-Adressen im Gegensatz zu IP-Adressen nichts über die Struktur des Netzes verraten, muß jede Bridge die MAC-Adresse aller Rechner im gesamten LAN kennen.

Somit hat man wieder das Problem, das man bei Routern vor der Einführung von Teilnetzen hatte: Mit wachsender LAN-Größe werden die Adreßtabellen der Bridges irgendwann gesprengt. Man kann also nicht beliebig viele LANs durch Bridges verbinden. Andererseits ermöglichen die unstrukturierten MAC-Adressen, daß die Bridges die Positionen von Rechnern im LAN automatisch anhand der empfangenen Pakete erlernen. Man nennt dies „selbstlernende Bridge".

DE

# 6 Technische Daten

## 6.1 Leistungs- und Kenndaten

| | *ELSA MicroLink Cable* | |
|---|---|---|
| **LAN-Schnittstelle** | Ethernet IEEE 802.3, 10Base-T (Twisted-Pair, RJ45, Node/Hub-Umschalter) | |
| **Netzwerkprotokolle** | Bridge-Betrieb | Bridging von allen IEEE-802.3-basierten Protokollen |
| | IP-Router | IP, TCP, ICMP, ARP, RIP-1, RIP-2, DHCP |
| **Filter-Möglichkeiten** | Bridge-Betrieb | Broadcast, Multicast, Ziel-MAC-Adresse, Quell-MAC-Adresse, automatische Filterung entsprechend lokaler bzw. ferner Stationen |
| | IP-Router | TCP-, UDP-Portfilterung, Quell- und Zielnetzfilter |
| **IP-Masquerading (NAT/PAT)** | Internet-Zugriff über eine IP-Adresse durch IP-Adreß- und Port-Umsetzung, Statische Adressierung oder dynamische Zuweisung der IP-Adresse über DHCP, Maskierung von TCP, UDP, ICMP und FTP, DNS-Forwarding, inverses Masquerading für IP-Dienste aus einem Intranet | |
| **Management** | Kabelnetzbetreiber | Über SNMP und TFTP (Übertragung von Konfigurationsdateien und Firmware-Updates) |
| | Anwender | Paßwortschutz, *ELSA LANconfig*, SNMP, TFTP, Telnet |
| **Anzeigen/Bedienung** | LEDs für LAN- und Kabelfernsehnetz-Status, Factory-Default-Taster, Reset-Taster | |
| **Stromversorgung** | 12 V AC mit Steckernetzteil für 230 V (US-Version: 110 V), 10 VA | |
| **Umgebungsbedingungen** | Temperatur: 5..40°C, Luftfeuchtigkeit: 0..80%, nicht kondensierend<br>Eine gute Belüftung des Gerätes muß gewährleistet sein! | |
| **Ausführung und Maße** | Stabiles Metallgehäuse, LEDs auf der Vorderseite, Anschlüsse auf der Rückseite, Abmessungen 158 x 32 x 135 mm (B x H x T) | |
| **Lieferumfang** | Zubehör | Steckernetzteil, F-auf-IEC169-2-Adapter, Anschlußkabel für Fernsehkabelnetz, 10Base-T-Kabel |
| | Software | Konfigurationssoftware *ELSA LANconfig*, TFTP-Client |
| | Dokumentation | Ausführliches Handbuch und *ELSA Cable Modem*-CD |
| **Service** | Garantie | 6 Jahre |
| | ELSAcare | Innerhalb von 100 Tagen ab Kauf erhalten Sie bei einem Garantiefall umgehend ein Neuprodukt |
| | Support | Über Hotline und Internet (www.elsa.de) |

DE

## 6.1.1 Kabel-TV-Schnittstelle DOCSIS

| *ELSA MicroLink Cable* | |
|---|---|
| DOCSIS (ITU-T J.112 B) | |
| Buchse | F-Buchse |
| Empfangsfrequenzband | 88–860 MHz |
| Empfangskanalbreite | 6 MHz |
| Empfangspegel | 48–78 dBµV |
| Empfänger-Modulation | 64QAM, 256QAM |
| Empfangsdatenrate (brutto) | 30,34 Mbit/s (64QAM)<br>42,88 Mbit/s (256QAM) |
| Signal-Rausch-Abstand in Empfangsrichtung | > 21 dB (64 QAM)<br>> 28 dB (256 QAM) |
| Sendefrequenzband | 5–42 MHz |
| Sendekanalbreite | 200–3200 kHz |
| Sendeleistung | -40,75 bis +9,25 dBm |
| Sender-Modulation | QPSK, 16QAM |
| Sendedatenrate | 0,32–5,12 Mbit/s (QPSK), 0,64–10,24 Mbit/s (16QAM) |
| Signal-Rausch-Abstand in Senderichtung | > 14 dB (Burst QPSK)<br>> 20 dB (Burst 16QAM) |

DE

## 6.1.2 Kabel-TV-Schnittstelle EuroDOCSIS

| *ELSA MicroLink Cable* | |
|---|---|
| EuroDOCSIS (ES 201 488, Physical Layer gemäß EN 300 429) | |
| Buchse | F-Buchse |
| Empfangsfrequenzband | 108–862 MHz |
| Empfangskanalbreite | 8 MHz |
| Empfangspegel | 43–77 dBµV |
| Empfänger-Modulation | 64QAM, 256QAM |
| Empfangsdatenrate (brutto) | 41,71 Mbit/s (64QAM)<br>55,61 Mbit/s (256QAM) |
| Signal-Rausch-Abstand in Empfangsrichtung | > 21 dB (64 QAM)<br>> 28 dB (256 QAM) |
| Sendefrequenzband | 5–65 MHz |
| Sendekanalbreite | 200–3200 kHz |
| Sendeleistung | -40,75 bis +9,25 dBm |
| Sender-Modulation | QPSK, 16QAM |
| Sendedatenrate | 0,32–5,12 Mbit/s (QPSK), 0,64–10,24 Mbit/s (16QAM) |
| Signal-Rausch-Abstand in Senderichtung | > 14 dB (Burst QPSK)<br>> 20 dB (Burst 16QAM) |

DE

# 7 Anhang

## 7.1 Konformitätserklärung

CE

### KONFORMITÄTSERKLÄRUNG

**DECLARATION OF CONFORMITY**

Diese Erklärung gilt für folgendes Erzeugnis:
This declaration is valid for the following product:

**Geräteart:** **Modem**
**Type of Device:**
**Typenbezeichnung:** ***MicroLink™ Cable***
**Product Name:**

Hiermit wird bestätigt, daß das Erzeugnis den folgenden Schutzanforderungen entspricht:
This is to confirm that this product meets all essential protection requirements relating to the

**Niederspannungs Richtlinie (73/23/EWG)**
**Low Voltage Directive (73/23/EEC)**
**EMV Richtlinie (89/336/EWG)**
**EMC Directive (89/336/EEC)**.

Zur Beurteilung der Konformität wurden folgende **Normen** herangezogen:
The assessment of this product has been based on the following **standards**

**EN 50082-1: 1992 Teile/Parts: EN61000-4-2,3,4,6,11**
**EN 50081-1: 1992 Teile/Parts: EN 55022B+A1: 1995 +A2: 1997**
**EN 60950: 1992+ A1: 1993 +A2: 1993 +A3: 1995 +A4: 1997 +A11: 1997**

Diese Erklärung wird verantwortlich für den Hersteller / Importeur
On behalf of the manufacturer / importer

**ELSA AG**
**Sonnenweg 11**
**D-52070 Aachen**

abgegeben durch
this declaration is submitted by

Aachen, 19. Juli 1999
Aachen, July 19th 1999

i.V. Peter Wieninger
Bereichsleiter Entwicklung
VP Engineering

DE

## 7.2 Allgemeine Garantiebedingungen

Diese Garantie vom 01.06.1998 gewährt die ELSA AG den Erwerbern von ELSA-Produkten nach ihrer Wahl zusätzlich zu den ihnen zustehenden gesetzlichen Gewährleistungsansprüchen nach Maßgabe der folgenden Bedingungen:

**1 Garantieumfang**

a) Die Garantie erstreckt sich auf das gelieferte Gerät mit allen Teilen. Sie wird in der Form geleistet, daß Teile, die nachweislich trotz sachgemäßer Behandlung und Beachtung der Gebrauchsanweisung aufgrund von Fabrikations- und/oder Materialfehlern defekt geworden sind, nach unserer Wahl kostenlos ausgetauscht oder repariert werden. Alternativ hierzu behalten wir uns vor, das defekte Gerät gegen ein Nachfolgeprodukt auszutauschen oder dem Käufer den Original-Kaufpreis gegen Rückgabe des defekten Geräts zu erstatten. Handbücher und evtl. mitgelieferte Software sind von der Garantie ausgeschlossen.

b) Die Kosten für Material und Arbeitszeit werden von uns getragen, nicht aber die Kosten für den Versand vom Erwerber zur Service-Werkstätte und/oder zu uns.

c) Ersetzte Teile gehen in unser Eigentum über.

d) Wir sind berechtigt, über die Instandsetzung und den Austausch hinaus technische Änderungen (z.B. Firmware-Updates) vorzunehmen, um das Gerät dem aktuellen Stand der Technik anzupassen. Hierfür entstehen dem Erwerber keine zusätzlichen Kosten. Ein Rechtsanspruch hierauf besteht nicht.

**2 Garantiezeit**

Die Garantiezeit beträgt für ELSA-Produkte sechs Jahre. Ausgenommen hiervon sind ELSA-Monitore und ELSA-Videokonferenzsysteme; hierfür beträgt die Garantiezeit drei Jahre. Die Garantiezeit beginnt mit dem Tag der Lieferung des Gerätes durch den ELSA-Fachhändler. Garantieleistungen bewirken weder eine Verlängerung der Garantiefrist, noch setzen sie eine neue Garantiefrist in Lauf. Die Garantiefrist für eingebaute Ersatzteile endet mit der Garantiefrist für das ganze Gerät.

**3 Abwicklung**

a) Zeigen sich innerhalb der Garantiezeit Fehler des Gerätes, so sind Garantieansprüche unverzüglich, spätestens jedoch innerhalb von sieben Tagen geltend zu machen.

b) Transportschäden, die äußerlich erkennbar sind (z.B. Gehäuse beschädigt), sind unverzüglich gegenüber der Transportperson und uns geltend zu machen. Äußerlich nicht erkennbare Schäden sind unverzüglich nach Entdeckung, spätestens jedoch innerhalb von sieben Tagen nach Anlieferung, schriftlich gegenüber der Transportperson und uns zu reklamieren.

c) Der Transport zu und von der Stelle, welche die Garantieansprüche entgegennimmt und/oder das instandgesetzte Gerät austauscht, geschieht auf eigene Gefahr und Kosten des Erwerbers.

d) Garantieansprüche werden nur berücksichtigt, wenn mit dem Gerät das Rechnungsoriginal vorgelegt wird.

**4 Ausschluß der Garantie**

Jegliche Garantieansprüche sind insbesondere ausgeschlossen,

a) wenn das Gerät durch den Einfluss höherer Gewalt oder durch Umwelteinflüsse (Feuchtigkeit, Stromschlag, Staub u.ä.) beschädigt oder zerstört wurde;

b) wenn das Gerät unter Bedingungen gelagert oder betrieben wurde, die außerhalb der technischen Spezifikationen liegen;

c) wenn die Schäden durch unsachgemäße Behandlung – insbesondere durch Nichtbeachtung der Systembeschreibung und der Betriebsanleitung – aufgetreten sind;

d) wenn das Gerät durch hierfür nicht von uns ermächtigte Personen geöffnet, repariert oder modifiziert wurde;

e) wenn das Gerät mechanische Beschädigungen irgendwelcher Art aufweist;

f) wenn Schäden an der Bildröhre eines ELSA-Monitors festgestellt werden, die insbesondere durch mechanische Belastungen (Verschiebung der Bildröhrenmaske durch Schockeinwirkung oder Beschädigungen des Glaskörpers), starke Magnetfelder in unmittelbarer Nähe (bunte Flecken auf dem Bildschirm), permanente Darstellung des gleichen Bildes (Einbrennen des Phosphors) hervorgerufen wurden;

g) wenn und soweit sich die Luminanz der Hintergrundbeleuchtung bei TFT-Panels im Laufe der Zeit allmählich reduziert;

h) wenn der Garantieanspruch nicht gemäß Ziffer 3a) oder 3b) gemeldet worden ist.

**5 Bedienungsfehler**

Stellt sich heraus, dass die gemeldete Fehlfunktion des Gerätes durch fehlerhafte Fremd-Hardware, -Software, Installation oder Bedienung verursacht wurde, behalten wir uns vor, den entstandenen Prüfaufwand dem Erwerber zu berechnen.

**6 Ergänzende Regelungen**

a) Die vorstehenden Bestimmungen regeln das Rechtsverhältnis zu uns abschließend.

b) Durch diese Garantie werden weitergehende Ansprüche, insbesondere solche auf Wandlung oder Minderung, nicht begründet. Schadensersatzansprüche, gleich aus welchem Rechtsgrund, sind ausgeschlossen. Dies gilt nicht, soweit z.B. bei Personenschäden oder Schäden an privat genutzten Sachen nach dem Produkthaftungsgesetz oder in Fällen des Vorsatzes oder der groben Fahrlässigkeit zwingend gehaftet wird.

c) Ausgeschlossen sind insbesondere Ansprüche auf Ersatz von entgangenem Gewinn, mittelbaren oder Folgeschäden.

d) Für Datenverlust und/oder die Wiederbeschaffung von Daten haften wir in Fällen von leichter und mittlerer Fahrlässigkeit nicht.

e) In Fällen, in denen wir die Vernichtung von Daten vorsätzlich oder grob fahrlässig verursacht haben, haften wir für den typischen Wiederherstellungsaufwand, der bei regelmäßiger und gefahrentsprechender Anfertigung von Sicherheitskopien eingetreten wäre.

f) Die Garantie bezieht sich lediglich auf den Erstkäufer und ist nicht übertragbar.

g) Gerichtsstand ist Aachen, falls der Erwerber Vollkaufmann ist. Hat der Erwerber keinen allgemeinen Gerichtsstand in der Bundesrepublik Deutschland oder verlegt er nach Vertragsabschluß seinen Wohnsitz oder gewöhnlichen Aufenthaltsort aus dem Geltungsbereich der Bundesrepublik Deutschland, ist unser Geschäftssitz Gerichtsstand. Dies gilt auch, falls Wohnsitz oder gewöhnlicher Aufenthalt des Käufers im Zeitpunkt der Klageerhebung nicht bekannt ist.

h) Es findet das Recht der Bundesrepublik Deutschland Anwendung. Das UN-Kaufrecht gilt im Verhältnis zwischen uns und dem Erwerber nicht.

DE

# 8 Index


- **A**
  - Adreß-Pool ... 56
  - Adreßverwaltung ... 54
  - Anzeigeelemente ... 9
  - Apple Talk ... 67
  - Ausschluß-Routen ... 46
- **B**
  - Betriebsarten ... 41
  - Bridge ... 53
    - Filterung von Datenpaketen ... 54
  - Broadcastadresse ... 69
  - Broadcast-Übertragung ... 74
  - Brute-Force ... 42
- **C**
  - Communities ... 38
- **D**
  - Datenpakete ... 65
  - DHCP ... 54
  - DHCP-Client ... 54
  - DHCP-Server ... 25, 55
  - Distanz einer Route ... 46
  - DNS ... 52
  - DNS-Forwarding ... 52
  - DNS-Server ... 54, 57
  - Domain Name Service ... 52
  - Dynamic Host Configuration Protocol 54
  - dynamisches Routing ... 45
- **E**
  - End-Adresse ... 56
- **F**
  - Filter ... 43
  - Firewall-Funktion ... 44
  - FirmSafe ... 35
  - Firmware-Upload ... 36
    - mit LANconfig ... 37
    - mit TFTP ... 37
  - Flash-ROM-Speicher ... 35
  - Funkstrecke ... 65
- **G**
  - Gateway ... 44, 54, 57
  - Gültigkeitsdauer ... 55, 57
- **H**
  - hierarchische IP-Adressen ... 71
  - Host ... 65
  - Hub ... 12
- **I**
  - IANA ... 70
  - Inband ... 25
    - mit Telnet ... 27
    - Voraussetzungen ... 25
  - Internet ... 44, 67
  - Internetwork ... 67
  - IP Masquerading ... 44
  - IP-Adresse ... 25, 44
  - IP-Adressen ... 68
  - IP-Masquerading ... 43, 49
    - einfaches Masquerading ... 51
    - unterstützte Protokolle ... 52
  - IP-Netz ... 67
  - IP-Routing
    - Filter ... 43
    - FTP ... 43
    - Telnet ... 43
  - IP-Routing-Tabelle ... 45
  - IPX ... 67
  - IP-Zugangsliste ... 25

DE


- **K**
  - Kabel ..... 65
  - Konfiguration
    - Befehle ..... 27
    - SNMP ..... 38
- **L**
  - LAN ..... 67, 74
  - LAN-Coll ..... 11
  - LANconfig ..... 25, 26, 36
  - LAN-Link ..... 11
  - LAN-Rx ..... 11
  - LAN-Tx ..... 11
  - LED ..... 9
  - Link-Status-LED ..... 12
  - Local Area Network ..... 67
  - Login ..... 36
  - Login-Sperre ..... 42
  - Login-Versuche ..... 42
  - lokales Netzwerk ..... 67
- **M**
  - MAC ..... 74
  - MAC-Adresse ..... 74
  - MAC-Protokoll ..... 74
  - Management-Information-Base ..... 40
  - Manager ..... 40
  - Medium ..... 64
  - Medium Access Control ..... 74
  - Mehrpunkt-Verkabelungen ..... 73
  - MIB ..... 39
  - Multiprotokollfähigkeit ..... 75
- **N**
  - NAT ..... 43, 44, 49
  - Network Information Center ..... 49
  - Netzmaske ..... 68
  - Netzwerk ..... 64
  - Netzwerkadresse ..... 68
  - Netzwerkkabel ..... 65
  - Netzwerkkarte ..... 64
  - Netzwerkprotokoll ..... 67
  - NIC ..... 49
  - Node ..... 12
- **O**
  - Objekte ..... 39
  - Online-Medien ..... 25
- **P**
  - Pakete ..... 65
  - Paßwortschutz ..... 41
  - PAT ..... 43, 44, 49
  - physikalisches Medium ..... 65
  - Port-Nr. ..... 51
  - Private Address Spaces ..... 70
  - Protokoll ..... 67
  - Punkt-zu-Mehrpunkt-Verbindung ..... 66
  - Punkt-zu-Punkt-Verbindung ..... 65
- **R**
  - registrierte IP-Adresse ..... 70
  - reservierte Adressbereiche ..... 70
  - Router ..... 65
  - Router-Name ..... 46
  - Routing ..... 71
  - Routingtabelle ..... 71
- **S**
  - Schnittstelle ..... 64
  - Shared Medium ..... 67, 74
  - Sicherheit ..... 41, 43, 44
  - Single User Access ..... 44
  - SNMP ..... 38
    - Agents ..... 38
    - Manager ..... 38
    - MIB ..... 39
  - Software einspielen ..... 35
  - Sperre ..... 42
  - Start-Adresse ..... 56

DE

statisches Routing ..... 45

- **T**

TCP/IP .....25, 45, 67
TCP/IP-Stack ..... 67
Technische Daten ..... 79
Teilnetz ..... 71
TFTP ..... 25
Trace
Beispiele ..... 35
Schlüssel und Parameter ..... 34
starten ..... 34
Trace-Ausgaben ..... 33
Trap ..... 40

- **U**

Upload ..... 36

- **V**

Verschlüsselung ..... 43

- **W**

WWW ..... 44

- **Z**

Zellen ..... 65
Zugangskontrolle ..... 42
Zugriffsprotokoll ..... 74